PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

17/SK

WP 252

Stanovisko č. 03/2017 k spracovaniu osobných údajov v kontexte kooperatívnych inteligentných dopravných systémov

Prijaté 4. októbra 2017

Obsah

Obsah

1 Úvod

Pracovnej skupine zriadenej podľa článku 29 bol 10. júla 2017 oficiálne predložený dokument „Spracovanie osobných údajov v kontexte kooperatívnych inteligentných dopravných systémov“ vypracovaný pracovnou skupinou pre ochranu údajov a súkromia v rámci platformy pre kooperatívne inteligentné dopravné systémy.

Platforma pre kooperatívne inteligentné dopravné systémy (ďalej len „kooperatívne IDS“) je iniciatívou Generálneho riaditeľstva Európskej komisie pre mobilitu a dopravu. Svoju činnosť začala na konci roka 2014 vytvorením špecializovaných pracovných skupín, ktoré sa zaoberajú rôznymi aspektmi zavedenia kooperatívnych IDS, od bezpečnosti, cez technickú štandardizáciu až po ochranu údajov.

Cieľom uvedeného dokumentu je poskytnúť podkladové informácie o spracovaní osobných údajov v kontexte kooperatívnych IDS a vyžiadať si usmernenie pracovnej skupiny zriadenej podľa článku 29 na účel posilnenia úrovne ochrany údajov v rámci týchto nových typov aplikácií.

Komisia pozvala delegátov pracovnej skupiny zriadenej podľa článku 29, aby sa pred predložením predmetného stanoviska zúčastnili na niekoľkých prípravných stretnutiach.

Pracovná skupina zriadená podľa článku 29 oceňuje príležitosť zapojiť sa do diskusie s príslušnými zainteresovanými stranami od raného štádia vývoja tejto novej technológie a v tejto súvislosti otvorí niektoré problémové otázky týkajúce sa všeobecného nariadenia o ochrane údajov, ktoré bude platným právnym rámcom v čase zavedenia kooperatívnych IDS.

Pracovná skupina zriadená podľa článku 29 víta nedávne uznesenie o ochrane údajov v automatizovaných a pripojených vozidlách prijaté na Medzinárodnej konferencii komisárov pre ochranu údajov a súkromia, ktorá sa konala v dňoch 25. – 29. septembra 2017 v Hong Kongu a potvrdzuje požiadavky, ktoré sú v tomto uznesení obsiahnuté.

2 Kooperatívne IDS

Kooperatívne IDS sú partnerským (angl. *peer-to-peer*) riešením určeným na výmenu údajov medzi vozidlami a inými zariadeniami cestnej infraštruktúry (dopravnými značkami alebo inými vysielacími/prijímacími základňovými stanicami) bez zásahu prevádzkovateľa siete.

Systém spočíva v tom, že partneri sa môžu navzájom priamo informovať o svojom postavení (prostredníctvom údajov zhromažďovaných snímačmi, ktorými sú vybavení), za čo získavajú podobné informácie. Takto sa (každému partnerovi) umožňuje vytvoriť si prehľad o stave prostredia okolo vozidla alebo zariadenia infraštruktúry. Očakáva sa, že na základe tejto komunikácie možno lepšie predpovedať dopravné situácie a zlepšiť prevenciu nehôd.

Kooperatívne IDS sú založené na nepretržitom vysielaní. Umožňujú komunikáciu *ad hoc*, pričom sa nevyžaduje vytvorenie trvalej komunikácie alebo spojení medzi partnermi.

V kontexte kooperatívnych IDS sa vymieňajú dva druhy správ: tzv. kooperatívne informačné správy (angl. *Cooperative Awareness Messages, CAM*), ktoré sa vysielajú kontinuálne a obsahujú údaje o pohybe a rozmery vozidla, a decentralizované notifikačné správy

o prostredí (angl. *Decentralised Environmental Notification Messages, DENM*), ktoré sa zasielajú nad rámec kooperatívnych informačných správ len pri výskyte konkrétnych naliehavých mimoriadnych udalostí (ako sú nehody) a obsahujú informácie o mieste udalosti. Kooperatívne informačné správy a decentralizované notifikačné správy o prostredí obsahujú šifrované podpisy, ktoré sú pre prijímajúcu stranu zárukou, že správy posiela spoľahlivý odosielateľ. Distribúcia certifikátov medzi partnermi sa uskutočňuje pomocou architektúry infraštruktúry verejného kľúča. Infraštruktúra verejného kľúča je riadiaca štruktúra, v ktorej je každý certifikát v konkrétnom čase jednoznačne spojený s vozidlom. Certifikát slúži na potvrdenie, že systém ho rozpoznáva a možno mu dôverovať.

Európska komisia už vo svojej stratégii kooperatívnych IDS identifikovala niekoľko prípadov použitia v rámci ich počiatočného zavedenia (aplikácie od prvého dňa). Tieto prípady, ktoré sú uvedené v dokumente pracovnej skupiny pre ochranu údajov a súkromia v rámci kooperatívnych IDS, súvisia väčšinou s informačnými funkciami (ako sú upozornenia na cestné práce, poveternostné podmienky atď.). Vodič má v týchto prípadoch použitia plnú kontrolu nad vozidlom a je zodpovedný za činnosť vozidla. Z dlhodobého hľadiska a pri vyššej úrovni automatizácie sa očakáva nárast vplyvu kooperatívnych IDS, keďže systém by mohol postupne prevziať rozhodnutia vodiča.

Pracovná skupina zriadená podľa článku 29 sa bude zameriavať výhradne na tieto počiatočné schopnosti aplikácií kooperatívnych IDS. Zavedenie vyšších úrovní automatizácie otvorí nové, veľmi dôležité otázky týkajúce sa vplyvu na slobodu a práva občanov EÚ. Pracovná skupina zriadená podľa článku 29 a následne aj Európsky výbor pre ochranu údajov posúdia tieto záležitosti v neskoršom štádiu. Pracovná skupina zriadená podľa článku 29 využíva túto príležitosť na to, aby podporila včasný dialóg medzi príslušnými zainteresovanými stranami o dôsledkoch týchto evolučných scenárov na ochranu údajov tým, že zohľadní aj zložité etické otázky súvisiace s týmto novým a hlbokým zásahom do tradične ľuďmi riadených činností.

3 Zhrnutie pracovného dokumentu o kooperatívnych IDS

3.1 Osobné údaje

Pracovná skupina pre ochranu údajov a súkromia v rámci kooperatívnych IDS uznáva, že vysielané správy, ktoré sa vymieňajú medzi vozidlami, sú osobné údaje. Tento záver vyplýva najmä z týchto dvoch pozorovaní: 1. správy obsahujú autorizačné certifikáty vydané infraštruktúrou verejného kľúča, ktoré sú jednoznačne spojené s odosielateľom; 2. správy obsahujú hlavičku, časové označenie, údaje o polohe a rozmery vozidla.

V predkladanom dokumente sa mechanizmus používaný na výmenu kooperatívnych informačných správ a decentralizovaných notifikačných správ o prostredí s ich digitálnymi certifikátmi vymedzuje ako spracovanie pseudonymizovaných údajov, a to s odôvodnením, že dodatočné informácie (spojenie medzi držiteľom certifikátu a údajmi o vozidle) sa uchovávajú oddelene od používateľa údajov (tieto informácie uchovávajú certifikačné orgány). Podľa článku 4 ods. 5 všeobecného nariadenia o ochrane údajov by na identifikáciu dotknutých osôb boli potrebné dodatočné informácie. Z tohto dôvodu sa podľa dokumentu má uplatniť článok 11 všeobecného nariadenia o ochrane údajov (spracúvanie bez potreby identifikácie). Dokument sa však netýka spracovania vykonávaného certifikačnými orgánmi a neobsahuje technické podrobnosti o infraštruktúre verejného kľúča, ktoré sú rozhodujúce na zabezpečenie pseudonymizácie vymieňaných údajov.

3.2 Právne dôvody

Pracovná skupina pre ochranu údajov a súkromia v rámci platformy pre kooperatívne IDS dospela k záveru, že zákonnosť spracovania nemusí byť založená iba na jednom právnom základe, ale na kombinácii dvoch alebo viacerých právnych základov, pri zohľadnení načasovania s ohľadom na zavedenie novej technológie v roku 2019. Pracovná skupina pre kooperatívne IDS sa súhrnne domnieva, že prípadnými vhodnými právnymi základmi alebo ich kombináciami, so zreteľom na povahu aplikácií poskytovaných od prvého dňa, môžu byť:

- verejný záujem [článok 6 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov],
- plnenie zmluvy [článok 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov],
- súhlas [článok 6 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov],
- oprávnený záujem [článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov].

Pracovná skupina pre kooperatívne IDS poznamenáva, že podmienkou uplatnenia verejného záujmu ako právneho základu je zakotvenie nevyhnutnosti takéhoto spracovania vo vnútroštátnom práve alebo práve Únie. To by mohlo byť súčasťou vykonávania stratégie EÚ v oblasti bezpečnosti cestnej premávky, účinnosti dopravy a trvalej udržateľnosti životného prostredia. V smernici 2010/40/EÚ o inteligentných dopravných systémoch sa Európskej komisii umožňuje prijať záväzné špecifikácie v tejto oblasti prostredníctvom delegovaných aktov. Pracovná skupina pre kooperatívne IDS považuje povinné zavedenie kooperatívnych IDS za možnosť, nie však v rámci počiatočného zavedenia v roku 2019.

Pracovná skupina pre kooperatívne IDS zvážila možnosť spracovania osobných údajov v prípade, že je to potrebné na splnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba. Podľa záverov, ku ktorým dospela pracovná skupina pre kooperatívne IDS, nemusí byť uplatniteľnosť tohto právneho základu všeobecná. Tento právny základ možno využiť v konkrétnych situáciách, napríklad keď dotknutá osoba skutočne uzatvorila zmluvu so súkromným správcom cesty, na základe ktorej môže po danej ceste jazdiť. Pracovná skupina pre kooperatívne IDS poznamenáva, že do kooperatívnych IDS je zapojený reťazec subjektov (výrobcovia automobilov, vývojári softvéru, správcovia ciest), ktorí môžu byť spoločnými prevádzkovateľmi v zmysle vymedzenia podľa článku 26 všeobecného nariadenia o ochrane údajov. Podmienkou právneho základu nevyhnutnosti splniť zmluvu je posúdenie úloh jednotlivých subjektov vo vzťahu k účelom a prostriedkom.

Pokiaľ ide o právny základ súhlasu, pracovná skupina pre kooperatívne IDS skúma technické obmedzenia vyplývajúce z vysielacej povahy komunikácie. V kontexte kooperatívnych IDS nemusia mať subjekty, ktoré plnia úlohu prevádzkovateľov, priamy individuálny vzťah s dotknutou osobou. Dotknutá osoba nevie a nemôže vedieť o všetkých príjemcoch svojich správ vzhľadom na spôsob, akým je táto norma navrhnutá [1]. Pracovná skupina pre kooperatívne IDS však navrhuje možnosť pripojiť k vysielaným kooperatívnym informačným

[1] ETSI EN 302 637-2 „Inteligentné dopravné systémy (IDS); Vozidlové komunikácie; Základný súbor aplikácií; Časť 2: Špecifikácia základnej služby kooperatívnej informovanosti“ a ETSI EN 302 637-3 „Inteligentné dopravné systémy (IDS); Vozidlové komunikácie; Základný súbor aplikácií; Časť 3: Špecifikácie základnej služby decentralizovaných notifikačných správ o prostredí“.

správam a decentralizovaným notifikačným správam o prostredí značky, do ktorých by bolo možné zakódovať používateľské preferencie.

Pracovná skupina pre kooperatívne IDS zvážila aj spracovanie na účel oprávnených záujmov prevádzkovateľa. Podmienkou využitia tohto právneho základu je, aby prevádzkovateľ zabezpečil, že spracovaním sa nenarušia záujmy alebo základné práva a slobody dotknutej osoby. Ako sa výslovne uvádza v dokumente, uplatniteľnosti tohto právneho základu bránia mnohé prekážky. Ide primárne o potrebu určiť, ktorý záujem sa uplatní v reťazci zodpovedností kooperatívnych IDS, vykonanie potenciálne oddelených testov vyváženosti zo strany každého zúčastneného subjektu v závislosti od ich úloh, a sekundárne o zavedenie ďalších osobitných záruk na obmedzenie neprimeraného vplyvu na dotknuté osoby.

4. Stanovisko pracovnej skupiny zriadenej podľa článku 29

4.1 Právny rámec

Počiatočné zavedenie kooperatívnych inteligentných dopravných systémov sa predpokladá v roku 2019. Príslušným právnym rámcom spracovania osobných údajov vo vzťahu ku kooperatívnym IDS je preto nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov), ktoré nadobudlo účinnosť 25. mája 2016 a ktoré bude uplatniteľné do 25. mája 2018.

Navyše, v budúcnosti môže byť potrebná nová smernica o súkromí a elektronických komunikáciách. Podľa návrhu Európskej komisie [COM(2017) 10][2] by mala komunikácia stroj-stroj patriť do rozsahu pôsobnosti uvedeného nariadenia.

4.2 Osobné údaje/identifikácia dotknutých osôb

Pracovná skupina pre kooperatívne IDS správne stanovila, že údaje prenášané cez kooperatívne IDS sú osobné údaje, pretože sa týkajú identifikovaných alebo identifikovateľných dotknutých osôb. Dotknuté osoby možno identifikovať rôznymi spôsobmi. Po prvé, prostredníctvom certifikátov poskytnutých infraštruktúrou verejného kľúča, keďže tieto certifikáty budú osobitne navrhnuté s cieľom odlíšiť vozidlo, v ktorom sú nainštalované. Po druhé, prostredníctvom samotných údajov o polohe, keďže možnosť identifikácie na základe týchto údajov je dobre známa[3]: len niekoľko bodov na ceste stačí na veľmi presnú identifikáciu jednotlivca v populácii, a to s ohľadom na väčšinou pravidelné modely mobility ľudí.

Platí to najmä pre kooperatívne informačné správy. Decentralizované notifikačné správy o prostredí obsahujú aj autorizačné doklady a údaje o konkrétnej udalosti. V závislosti od spôsobu, akým sa udalosť odohrala (napr. neobývanosť oblasti, konkrétny čas dňa alebo dynamika reťazca udalostí), môže byť dotknutá osoba identifikovaná aj na základe týchto správ.

[2] Legislatívny návrh Európskej komisie COM(2017) 10 o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách (smernica o súkromí a elektronických komunikáciách), január 2017. Pozri aj stanovisko pracovnej skupiny zriadenej podľa článku 29, WP247, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

[3] Stanovisko pracovnej skupiny zriadenej podľa článku 29 č. 05/2014 k technikám anonymizácie, WP X.

Pokiaľ ide o uplatniteľnosť článku 11 všeobecného nariadenia o ochrane údajov, pracovná skupina zriadená podľa článku 29 by rada vzniesla tieto obavy. V článku 11 sa stanovuje, že existujú operácie spracovania, pri ktorých nie je potrebná alebo už nie je potrebná identifikácia dotknutej osoby a prevádzkovateľ nie je povinný zisťovať totožnosť dotknutej osoby výlučne na účel súladu so všeobecným nariadením o ochrane údajov. Tento článok by sa mal vykladať ako nástroj na presadenie „skutočnej“ minimalizácie údajov, avšak bez toho, aby sa bránilo výkonu práv dotknutých osôb. Výkon týchto práv sa musí umožniť pomocou „dodatočných informácií“ poskytnutých dotknutou osobou. Odvolaním sa na článok 11 všeobecného nariadenia o ochrane údajov bez určenia ďalších údajov potrebných na identifikáciu dotknutých osôb sa *de facto* zabraňuje výkonu práv dotknutých osôb (na prístup, nápravu, prenosnosť atď.). Pseudonymizované údaje sa však vymedzujú ako osobné údaje (pozri článok 4 všeobecného nariadenia o ochrane údajov), lebo ide o údaje týkajúce sa identifikovateľnej osoby (pozri najmä odôvodnenie 26 všeobecného nariadenia o ochrane údajov).

Pracovná skupina zriadená podľa článku 29 preto vyzýva, aby pracovná skupina pre kooperatívne IDS predložila návrhy týkajúce sa pojmu „dodatočných informácií“ v kontexte tejto novej služby s cieľom zabezpečiť účinnosť tohto nariadenia, pri zohľadnení napríklad konkrétnych údajov o vozidle alebo vysokej pravdepodobnosti identifikácie na základe údajov o polohe. Pracovná skupina odmieta akýkoľvek výklad článku 11 zameraný na zníženie zodpovednosti kontrolóra(-ov) za dodržanie povinností súvisiacich s ochranou údajov.

Osobné údaje spracúvané v kooperatívnych IDS môžu zahŕňať aj osobitné kategórie údajov v zmysle vymedzenia podľa článku 10 všeobecného nariadenia o ochrane údajov súvisiace s porušením signálu (napríklad v dokumente uvedené „porušenie signálu/bezpečnosť križovatky“). Tieto osobitné kategórie údajov môžu byť spracované v kooperatívnych IDS a vysielané do iných vozidiel. V článku 10 všeobecného nariadenia o ochrane údajov sa stanovuje, že údaje týkajúce sa odsúdení a trestných činov možno spracovávať len pod kontrolou orgánu verejnej moci, alebo ak je spracúvanie povolené právom Únie či právom členského štátu poskytujúcim primerané záruky práv a slobôd dotknutých osôb. V dôsledku toho by sa mali aplikácie od prvého dňa modifikovať tak, aby sa zabránilo zhromažďovaniu a šíreniu akýchkoľvek informácií, na ktoré by sa mohol vzťahovať článok 10.

Pracovná skupina vidí niekoľko technických možností na minimalizáciu rizík opätovnej identifikácie.

Po prvé, môže sa zlepšiť politika vydávania certifikátov v rámci infraštruktúry verejného kľúča. Pokiaľ je certifikát platný, vozidlo možno identifikovať a sledovať, pričom sledovanie na krátke vzdialenosti je dôležitou súčasťou dizajnu kooperatívnych IDS. Sledovanie na krátku vzdialenosť umožňuje tesné príčinné spojenie medzi podmienkami na cestách a vozidlami pohybujúcimi sa v danej oblasti, a preto sa považuje za nevyhnutnú podmienku fungovania systému a aplikácií. S cieľom zabrániť dlhodobému sledovaniu, ktoré nie je nevyhnutné pre bezpečnosť cestnej premávky, sa autorizačné doklady v čase menia. Hoci pracovná skupina pre kooperatívne IDS zdôrazňuje potrebu nízkej frekvencie zmien autorizačných dokladov, aby sa obmedzila spotreba certifikátov a aby sa neznemožnila jednoduchá identifikácia nebezpečenstiev a varovaní o vodičoch jazdiacich v blízkosti, pracovná skupina zriadená podľa článku 29 odporúča starostlivo posúdiť možnosti vyššej frekvencie s cieľom obmedziť riziká dlhodobého sledovania.

Po druhé, je potrebné upraviť frekvenciu vysielania kooperatívnych informačných správ.
Podľa navrhovaného nastavenia frekvencie kooperatívnych informačných správ by bolo možné sledovať vozidlá v rozmedzí niekoľkých metrov. Možno to urobiť napríklad tak, že rôzne segmenty veľmi hustých sekvencií časovo označených bodov, ktoré môžu byť umiestnené napríklad na mape, budú „farebne“ odlíšené osobitným certifikátom (za predpokladu, že každý certifikát bude vizuálne označený inou farbou). Pracovná skupina pre kooperatívne IDS vo svojom dokumente tvrdí, že „farebným odlíšením“ uvedených segmentov na mape (t. j. pripojením rôznych certifikátov k týmto segmentom) sa pozorovateľovi zabráni zostaviť celú cestu vozidla, čo je však otázne. Údaje o mobilite sú inherentne a výrazne korelované a pri väčšine vodičov značne repetitívne. Pre útočníka s prostriedkami a motiváciou by sa zosúladenie zjavne nesúvisiacich segmentov na trase vedúcej z bodu do bodu nemalo vnímať ako neprimerané. Okrem toho, keď vozidlo zmení svoj certifikát, bude naďalej možné prepojiť starý a nový certifikát: akékoľvek iné vozidlo v blízkosti vozidla, ktoré zmenilo svoj certifikát, bude môcť sledovať zmiznutie starého certifikátu a objavenie sa nového, a tak ich bude môcť prepojiť. Pracovná skupina pre

kooperatívne IDS by sa mala touto otázkou zaoberať s cieľom zabrániť podobných koreláciám.

Po tretie, pracovná skupina zriadená podľa článku 29 zdôrazňuje význam zásady minimalizácie údajov s cieľom zmierniť riziko opätovnej identifikácie, a to aj prostredníctvom uplatňovania nápravných opatrení, ako je zovšeobecnenie alebo rušenie[4]. Takéto nápravné opatrenia môžu byť navrhnuté tak, aby neovplyvnili celkový obraz stavu prostredia a možnosť identifikovať nové nebezpečenstvo, ale aby obmedzili zbytočné vystavenie alebo dlhodobé sledovanie vodiča. Zvláštna pozornosť by sa mala venovať zovšeobecneniu alebo rušeniu vo vzťahu k statickým vlastnostiam vozidiel s cieľom minimalizovať riziko sledovania prostredníctvom individuálnych vlastností vozidiel.

4.3 Riziká pre ochranu súkromia

Pracovná skupina zriadená podľa článku 29 uznáva, že kooperatívne IDS môžu vodičom priniesť výhody vyplývajúce z vyššej úrovne využiteľnosti a informovanosti o prostredí. Pre verejnosť môžu byť prospešné prostredníctvom zlepšenia bezpečnosti na cestách a ochrany bezpečnosti ostatných vodičov a chodcov. Pracovná skupina zriadená podľa článku 29 však zdôrazňuje, že rozsiahle zavádzanie tejto novej technológie, ktorá bude zahŕňať zber a spracovanie bezprecedentného množstva údajov o polohe jednotlivcov v Európe, prináša nové výzvy v oblasti základných práv a ochrany osobných údajov a súkromia používateľov, ako aj iných osôb, na ktoré môže mať vplyv.

Po prvé, základom kooperatívnych IDS je odhalenie toho, čo sme nezvykli zverejňovať: kde šoférujeme a ako šoférujeme. Prostredníctvom vysielacích a prijímacích schopností vozidiel sa tieto intímne informácie budú verejne vysielať na akékoľvek blízke vozidlo. Ide o formu distribuovaného trvalého sledovania správania, ktoré môže vyvolať nepríjemný pocit tajného sledovania.

Ďalším významným rizikom z hľadiska ochrany súkromia je nedostatočná transparentnosť. Prostredníctvom svojich vozidiel sa používatelia stanú trvalými vysielateľmi. Musia si byť plne vedomí rozsahu spracovania a ostatných partnerov, s ktorými si vymieňajú údaje v prostredí kooperatívnych IDS (ostatné vozidlá, výrobcovia automobilov, správcovia ciest, iné verejné alebo súkromné subjekty), a spôsobov, akými údaje spracúvajú.

Výber vysielania medzi partnermi ako kanála na distribúciu správ, namiesto komunikácie jedného na jedného, predstavuje ďalšiu výzvu: správy môže prijímať neobmedzený počet subjektov, ktorých zámery a technologické kapacity nie sú a nemôžu byť odosielateľovi známe. To spôsobuje informačnú asymetriu medzi odosielateľmi a ostatnými partnermi (príjemcami) kooperatívnych IDS. Táto asymetria sa musí vyvážiť vyššou úrovňou kontroly osobných údajov.

Údaje o pohybe a polohe budú veľmi cenné pre mnohé zainteresované strany s rôznymi zámermi a účelmi, od inzerentov až po výrobcov automobilov a poisťovne. Neobmedzený a nediskriminačný prístup k údajom zdieľaným v rámci kooperatívnych IDS môže umožniť nekalé zhromaždenie individuálnych pohybových profilov a „datifikáciu“ vodičského správania, na základe ktorých sa môžu vytvárať, propagovať a predávať personalizované tovary a služby.

[4] Pozri príklady uvedené v stanovisku pracovnej skupiny podľa článku 29 č. 05/2014 k technikám anonymizácie, WP 216.

Údaje o mobilite môžu byť atraktívne aj v súvislosti s presadzovaním práva a dopravnej bezpečnosti nad rámec účelu, na ktorý sa údaje z kooperatívnych IDS generujú a spracúvajú. To vyvoláva obavy týkajúce sa nevyhnutnosti a primeranosti, pokiaľ ide o ich potenciálne využitie na tieto iné účely.

Ďalším objavujúcim sa rizikom týkajúcim sa ochrany údajov v rámci kooperatívnych IDS je rozširovanie využitia technológie mimo pôvodne zamýšľaného účelu. Ak sa informačná asymetria týkajúca sa totožnosti ostatných partnerov, ktorá je inherentnou vlastnosťou danej vysielacej architektúry, nebude vhodne riešiť nástrojmi na vybudovanie dôvery, môže spôsobiť skreslenie pôvodného rozsahu komunikácie a presmerovať používateľov na neplánované miesta. Dôvodom môžu byť nepresné predpovede o stave prostredia (napr. vytváranie dopravnej zápchy namiesto zníženia dopravného zaťaženia) alebo dokonca na základe takého výkladu údajov o prostredí, ktorý nie je neutrálny (napr. nabádanie používateľov, aby navštívili konkrétne oblasti z dôvodu hospodárskych záujmov jedného z partnerov).

4.4 Zákonnosť spracovania

Treba zdôrazniť, že nariadenie (EÚ) 2016/679 sa nevzťahuje na spracovanie osobných údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti [článok 2 (2) (c)]. Táto výnimka sa môže uplatniť len v prípade, ak je prísne obmedzená na spracovanie, ktoré sa uskutočňuje vnútri vozidla, a to iba vtedy, keď má vodič úplnú kontrolu nad spracovaním vo svojom zariadení. Nemôže platiť, keď zariadenie inštalované v autách posiela údaje iných blízkych automobilov, či už okamžite, alebo v dôsledku lokálneho spracovania. V takýchto prípadoch sa spracovanie netýka výlučne osobnej činnosti.

Zákonnosť spracúvania osobných údajov v rámci fungovania kooperatívnych IDS sa vyžaduje podľa článku 6 ods. 1 všeobecného nariadenia o ochrane údajov. Spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok: a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely; b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba; c) spracúvanie je potrebné na splnenie zákonnej povinnosti prevádzkovateľa; d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby; e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi; f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby.

Vzhľadom na cieľ kooperatívnych IDS, ktorým je zlepšenie bezpečnosti na cestách, podpora účinnosti dopravy a podpora environmentálnej udržateľnosti, a to aj prostredníctvom zavedenia tohto interoperabilného celoeurópskeho systému, pracovná skupina zriadená podľa článku 29 konštatuje, že dlhodobým právnym základom pre tento typ spracovania je prijatie právneho nástroja na úrovni EÚ [článok 6 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov]. Je pravdepodobné, že vzhľadom na plánovanú prevalenciu (čiastočne) autonómnych vozidiel sa zavedenie tejto technológie do vozidiel stane časom povinným, čo je porovnateľné s právnou povinnosťou výrobcov automobilov zaviesť funkciu eCall do všetkých nových vozidiel. Takouto právnou povinnosťou by sa nemal umožniť plošný zber a spracovanie osobných údajov. Rozsah právnej povinnosti musí byť riadne posúdený a potvrdený ako

primeraný a nevyhnutne potrebný v demokratickej spoločnosti, tak ako sa to vyžaduje v rámci ochrany poskytovanej uplatniteľnými základnými právami.

Komisia by mala čo najskôr iniciovať tento proces posúdenia a tvorby právnych predpisov, aby sa zabránilo tomu, že spracovanie údajov o polohe a iných osobných údajoch občanov EÚ v rámci kooperatívnych IDS sa uskutoční bez právneho základu a nebude plne pokryté primeranou úrovňou ochrany.

V rámci analýzy ostatných právnych základov chýbajú niektoré dôležité prvky. Užitočné by mohlo byť posúdiť technické možnosti kooperatívnych IDS a rozsah ich pôsobnosti.

Sledovanie polohy, rýchlosti a smeru vozidla je podstatou kooperatívnych IDS. Čím vyššia je frekvencia vymenených správ, tým presnejší a podrobnejší je prehľad o prostredí okolo vozidiel a tým lepšia je schopnosť systému predpovedať nebezpečenstvo. Pracovná skupina zriadená podľa článku 29 chápe, že miera prijatia a prispievania údajmi je rozhodujúcim faktorom na fungovanie kooperatívnych IDS: nízka úroveň prispievania údajmi alebo nízke rozlíšenie prehľadu o prostredí zachytené jednotlivými vozidlami by mohlo ovplyvniť alebo dokonca poškodiť platnosť kooperatívnych IDS ako nástroja bezpečnosti cestnej premávky.

Spustenie prijatia však nepredstavuje nútenie do všadeprítomného sledovania. Možnosť využívať kooperatívne IDS by *per se* mala vodičov motivovať, aby sa ich slobodne pridržiavali. V takom prípade môže dôjsť k prirodzenému získaniu kritického množstva používateľov, čo umožní správne fungovanie systému bez akejkoľvek povinnosti. Ľuďom sa pritom ponechá možnosť slobodne si vybrať, či sa chcú na systéme zúčastniť, a ak áno, vybrať si možnosti sledovania (časovanie, frekvencia, polohy), ktoré najlepšie zodpovedajú ich preferenciám.

Úroveň rozlíšenia pri sledovaní sa dobre vyjadruje ukazovateľmi výkonnosti systému[5]:

„*Vozidlo vytvorí správu kooperatívnej informovanosti približne každé 4 metre, a keď zmení smer jazdy o viac ako 4°. Keď sa zmení vzdialenosť medzi aktuálnou a predchádzajúcou pozíciou o viac ako 4 metre alebo ak sa rýchlosť zmení o viac ako 0,5 m/s v porovnaní s naposledy odoslanou správou kolektívnej informovanosti, ale za normálnych podmienok najmenej raz za sekundu a najviac raz za 0,1 sekundy.*“

Tieto možnosti sledovania predstavujú základnú úroveň. Ako sa uvádza v dokumente, v skutočnosti ide o „*aktuálne vymedzené špecifikácie, ktoré sa môžu meniť podľa aktuálnych potrieb súvisiacich s novými funkciami*“. Podľa dokumentu nemôže používateľ tieto nastavenia zmeniť. Pracovná skupina pre kooperatívne IDS v tomto prípade stanovila nesprávnu rovnováhu medzi potrebou podporiť prijímanie kooperatívnych IDS a potrebou zabrániť „parazitovaniu“ osôb, ktoré sa na nich nepodieľajú, ale využívajú ich výhody, a to stanovením frekvencie výmeny správ (a teda aj úrovne podrobnosti sledovania) na najvyššej možnej úrovni.

Pracovná skupina pre kooperatívne IDS zatiaľ nedosiahla konsenzus o technickej uskutočniteľnosti získania súhlasu. Pracovná skupina zdôrazňuje, že je potrebné naplniť všetky prvky platného súhlasu tak, ako sa uvádza v článku 7 všeobecného nariadenia o ochrane údajov a odôvodnenia 42. Prevádzkovatelia musia venovať osobitnú pozornosť podmienkam získania konkrétneho, bezplatného a informovaného súhlasu od rôznych

[5] Spracovanie osobných údajov v kontexte kooperatívnych IDS: Príloha I – Aplikácie od prvého dňa, normy a bezpečnosť (A.2.2 Správy kooperatívnej informovanosti).

účastníkov, ako sú vlastníci alebo používatelia áut. Takýto súhlas musí byť poskytnutý samostatne na konkrétny účel, nesmie byť spojený so zmluvou o kúpe alebo prenájme nového vozidla a musí byť rovnako ľahko odvolateľný, ako bol poskytnutý. Súhlas navyše nie je primeraným právnym základom, pokiaľ ide o zamestnancov, keďže vzťah zamestnávateľ – zamestnanec sa vyznačuje právnym podriadením a zamestnanci nemôžu slobodne odmietnuť súhlas.

Najmä preto, že kooperatívne IDS sú založené na nepretržitom vysielaní, neexistuje žiadny bod prerušenia vysielania, ktorý by slúžil na signalizovanie úmyslu alebo želania na strane užívateľa. Vysielanie je navyše výlučne dopredu orientovanou komunikačnou schémou bez akéhokoľvek spätného účinku, čo znemožňuje nastaviť mechanizmus vzájomného uznávania medzi dotknutou osobou (odosielateľom) a prevádzkovateľom (príjemcom). Toto nedostatočné vzájomné uznávanie samo osebe nebráni použitiu súhlasu, sťažuje však spracovanie údajov výhradne na konkrétne a presne vymedzené účely známymi prevádzkovateľmi. Na druhej strane tvrdenie uvedené v dokumente, že súhlas nemožno považovať za účinný právny základ, lebo prevádzkovateľ v tomto štádiu nebol vymedzený na úrovni, ktorá by dotknutej osobe umožnila zistiť jeho totožnosť, je zavádzajúce: existencia dobre vymedzeného(-ých) prevádzkovateľa(-ov) je predpokladom samotného spracovania, pričom článok 6 ods. 1 všeobecného nariadenia o ochrane údajov neposkytuje právny základ, ktorým by sa mohla odôvodniť nejasnosť jeho totožnosti. Technická snaha o zaradenie značiek do štruktúry správ kooperatívnej informovanosti a decentralizovaných notifikačných správ o prostredí s cieľom signalizovať preferencie používateľov je dobrým východiskovým bodom, ale zatiaľ nie je riešením.

Pracovná skupina pre kooperatívne IDS sa zaoberá aj možnosťou spoliehať sa na potrebu plniť zmluvu [článok 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov]. Osobitná zmluva medzi dotknutou osobou a prevádzkovateľom, ktorá je oddelená od akýchkoľvek iných zmlúv o kúpe/lízingu, by v zásade mohla vodičovi umožniť slobodne sa pridržiavať systému.

Pokiaľ ide o uplatniteľnosť možnosti spoločného prevádzkovania uvedenú v článku 26 všeobecného nariadenia o ochrane údajov, treba zdôrazniť, že nejde o súťaž medzi spoločnými prevádzkovateľmi, ani o to, aby sa poskytla možnosť čiastočne alebo úplne obísť povinnosti prevádzkovateľov. Spoloční prevádzkovatelia, ktorí majú ustálený vzťah so zákazníkmi alebo jednotlivcami a môžu s nimi priamo komunikovať, by mali prevziať plnú zodpovednosť za informovanie o reťazci zodpovednosti, existencii a cieľoch ostatných spoločných prevádzkovateľov.

V prípade, že je spracovanie nevyhnutné na vykonanie konkrétnej a slobodne zvolenej zmluvy, ktorej je dotknutá osoba stranou, pracovná skupina zriadená podľa článku 29 opakovane uviedla[6], že toto ustanovenie sa musí vykladať striktne a že existuje jasná súvislosť medzi posúdením nevyhnutnosti a dodržiavaním zásady obmedzenia účelu. V kontexte kooperatívnych IDS majú prvoradý význam dva aspekty. Po prvé, je dôležité vopred jasne určiť strany podieľajúce sa na zmluve s cieľom obmedziť spracovanie na limitovaný súbor jediných aktérov v rámci kooperatívnych IDS a zabrániť akémukoľvek ďalšiemu využívaniu neznámymi tretími stranami. Príklad uvedený v dokumente týkajúci sa zmluvy medzi dotknutými osobami a súkromnými prevádzkovateľmi cesty je neúplný, pretože do spracovania môžu byť zapojené aj iné strany (napríklad výrobcovia automobilov a vývojári softvéru) – buď ako spoloční prevádzkovatelia podľa článku 26 všeobecného

[6] Stanovisko č. 02/2013 k aplikáciám v inteligentných zariadeniach a stanovisko č. 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES.

nariadenia o ochrane údajov, alebo ako celok v kontexte jediného konzorcia, ktoré má úlohu plného prevádzkovateľa – a ktoré môžu uzavrieť zmluvu s dotknutými osobami. Po druhé, odôvodnenie zmluvy, jej predmet a ciele musia predchádzať samotnému spracovaniu a prevádzkovateľ(-lia) musia na základe tohto odôvodnenia a cieľov odskúšať, či je spracovanie údajov nevyhnutné na plnenie zmluvy s každým jednotlivým používateľom s ohľadom na to, že autá môžu riadiť ich majitelia alebo iní používatelia.

Pokiaľ ide o prípadné uplatnenie potreby spracovať údaje na základe oprávneného záujmu [článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov], pracovná skupina zriadená podľa článku 29 pripomína, že by sa to nemalo považovať za „poslednú možnosť“ v zložitých prípadoch, kde sa ťažko uplatňujú iné dôvody zákonného spracovania. Na základe výsledku testu vyváženosti by sa mohlo určiť, či článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov možno považovať za právny základ spracovania. Ako sa uvádza v dokumente, predpokladom je identifikácia prevádzkovateľov a ich záujmov. Treba však zvážiť ďalšie relevantné faktory[7]. Predovšetkým zdroj oprávnenosti záujmu (či už je založený na verejnom záujme alebo na obchodnom záujme konkrétnej strany), vplyv na dotknuté osoby a ich očakávania týkajúce sa ochrany súkromia, a to aj vzhľadom na potenciálne citlivú povahu údajov o polohe, dodatočné (aj technické) záruky, ktorými by sa mohol obmedziť akýkoľvek neprimeraný vplyv na ne.

4.5 Bezpečnosť

Kooperatívne IDS sú založené na vysielaní správ. Zabezpečenie dôvernosti, integrity a dostupnosti komunikácie, t. j. bezpečnosti komunikácie, si v tejto súvislosti vyžaduje osobitné úsilie a špecifikácie v porovnaní s komunikáciou jeden na jedného.

Vysielanie je neobmedzeným spôsobom komunikácie s neznámymi prijímajúcimi stranami v dosahu vysielajúceho zariadenia. Akýkoľvek zmysluplný spôsob obmedzenia spracovania vysielaných informácií iba na kontext aplikácie kooperatívnych IDS prostredníctvom zamedzenia neoprávneného spracovania týchto informácií prijímajúcou stranou, ktorá nie je kooperatívnym IDS, sa teda bude opierať o existenciu dôveryhodných partnerov a o skutočnosť, že použitie údajov pochádzajúcich z kooperatívnych IDS na iné účely ako bezpečnosť na cestách by bolo trestným činom.

Treba pripomenúť, že legislatívny návrh smernice o súkromí a elektronických komunikáciách, COM(2017) 10, obsahuje veľmi prísne obmedzenia týkajúce sa používania „emitovaných údajov“, ako sú správy kooperatívnej informovanosti a decentralizované notifikačné správy o prostredí, pričom v článku 8 ods. 2 sa stanovuje všeobecný zákaz ich používania. Výnimkou sú prípady, keď sa to robí výlučne na čas potrebný na vytvorenie spojenia a na zavedenie vhodných technických a organizačných opatrení na zaistenie úrovne bezpečnosti zodpovedajúcej rizikám, ako sa uvádza v článku 32 všeobecného nariadenia o ochrane údajov.

V dokumente sa kladie osobitný dôraz na mechanizmus infraštruktúry verejného kľúča ako spôsobu vybudovania dôvery v systém kooperatívnych IDS. Infraštruktúra verejného kľúča je vlastne spôsob, ako presadiť distribúciu konkrétneho informačného zdroja (v prípade kooperatívnych IDS digitálnych certifikátov) v rámci kontrolovanej štruktúry riadenia. Infraštruktúra verejného kľúča neobsahuje žiadny mechanizmus presadenia s cieľom určiť

[7] Stanovisko č. 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES.

skutočné zámery držiteľov alebo emitentov certifikátov. Žiaľ, v posledných rokoch narástol počet kolúzií alebo bezpečnostných incidentov ovplyvňujúcich certifikačné orgány a existujú silné stimuly na získanie certifikácií len na účely páchania škodlivých činov[8].

Existenciou architektúry infraštruktúry verejného kľúča sa *per se* nezaručuje vytvorenie vzťahu dôvery medzi partnermi. Na posilnenie dôvery sú potrebné ďalšie dodatočné opatrenia. Dôležitým prvkom je zavedenie mechanizmov na zaručenie bezpečnosti. Ďalšie relevantné faktory sa týkajú dôkladnej a pravidelnej kontroly činnosti certifikačných orgánov buď formou krížovej kontroly medzi certifikačnými orgánmi, alebo prostredníctvom auditov či inšpekcií vykonávaných verejnými inštitúciami, ktoré sa podieľajú na rozvoji kooperatívnych IDS.

Zabezpečenie integrity znamená zabrániť tomu, aby sa údaje mohli neoprávneným spôsobom zmeniť, čím by sa narušilo správne fungovanie informačného systému. V kontexte vysielania kooperatívnych IDS môže takáto situácia nastať, ak partneri (dokonca aj dôveryhodní partneri) manipulujú s obrazom okolitého prostredia tým, že tajne vkladajú falošné údaje, alebo sledujú skôr obchodný záujem ako verejný cieľ bezpečnosti cestnej premávky. Filtrovanie extrémnych hodnôt v prúde správ kooperatívnej informovanosti a decentralizovaných notifikačných správ o prostredí, ktoré by mohli vykazovať iné ako priemerné ukazovatele, je platným odstrašujúcim mechanizmom proti škodlivému používaniu kooperatívnych IDS a spôsobom, ako zabezpečiť, aby sa vymieňali tie údaje, ktoré sú na tento účel nevyhnutné.

Dostupnosť je schopnosť informácií slúžiť svojmu účelu, keď je to potrebné. V prostredí vysielania sa táto vlastnosť veľmi zložito zaručuje, a to z dôvodu kompromisu medzi časom a kvalitou údajov. Ak by údaje súvisiace s potenciálnym nebezpečenstvom (a teda ich dostupnosť) vznikli súbežným, masívnym vysielaním správ o tejto situácii, spoliehanie sa na príliš malú vzorku správ by mohlo viesť k mnohým falošným poplachom; na druhej strane vzhľadom na bezpečnosť ľudí niekedy nie je možné čakať na získanie dostatočného množstva dôkazov z mnohých rôznych zdrojov. Prevencia nehôd je veľmi dôležitý výsledok, ktorý sa očakáva od spracovania osobných údajov v kontexte kooperatívnych IDS, a pracovná skupina zriadená podľa článku 29 odporúča vývojárom softvéru, aby venovali maximálnu pozornosť a úsilie navrhnutiu softvérových programov schopných rozlíšiť falošné kladné a negatívne informácie, a to aj prostredníctvom spoločnej aktualizácie parametrov služby tak, aby sa nevytvárali poplašné signály, alebo naopak, aby sa zabránilo vzniku skutočne nebezpečných situácií pre dotknuté osoby.

5 Požadované opatrenia

Pracovná skupina zriadená podľa článku 29 víta úsilie Európskej komisie a pracovnej skupiny pre ochranu údajov a súkromia v rámci kooperatívnych IDS od začiatku začleniť zásady ochrany údajov do fungovania týchto nových aplikácií.

Posúdenie vykonané pracovnou skupinou pre kooperatívne IDS je dobrým východiskovým bodom, je však potrebné doplniť ho množstvom konkrétnych opatrení na rôznych úrovniach. Pracovná skupina zriadená podľa článku 29 považuje za osobitne dôležité najmä ďalej uvedené aspekty ochrany údajov.

[8] Edelman, Benjamin. „Nepriaznivý výber pri online certifikátoch ‚dôvery' a výsledkoch vyhľadávania." Výskum a aplikácie elektronického obchodu 10, č. 1 (január – február 2011).

- Komisia by mala zaviesť predpisy týkajúce sa zberu a spracovania údajov v oblasti inteligentných dopravných systémov pre jednotlivé sektory.
- Komisia by mala pripraviť plán zákonného spracovania údajov o polohe občanov EÚ v súvislosti s aplikáciami kooperatívnych IDS, pričom konečným cieľom je prijatie právneho nástroja v celej EÚ [článok 6 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov].
- Prijatie týchto právnych nástrojov by sa malo začať posúdením nevyhnutnosti a primeranosti ich ustanovení. Do legislatívneho procesu by sa navyše malo zaviesť povinné posúdenie vplyvu ochrany údajov (článok 35 ods. 10 všeobecného nariadenia o ochrane údajov), aby sa od začiatku objasňovali riziká a zmierňujúce opatrenia.
- Ďalšie právne základy uvedené v dokumente pracovnej skupiny pre kooperatívne IDS (konkrétne súhlas, výkon oprávneného záujmu dodávateľa) možno využiť len vtedy, ak sa pri každom z nich vyriešia kritické problémy identifikované v tomto stanovisku.
- Pri všetkých vybratých právnych základoch musí byť predvolené nastavenie všetkých nainštalovaných funkcií kooperatívnych IDS „vypnuté“.
- Treba vykonať ustanovenia článku 25 všeobecného nariadenia o ochrane údajov (Špecificky navrhnutá a štandardná ochrana údajov), čo používateľom umožní zvoliť si možnosti sledovania (načasovanie, frekvencia, polohy), ktoré najlepšie vyhovujú ich preferenciám.
- Treba posilniť bezpečnosť s cieľom obmedziť riziko nezákonného používania údajov z kooperatívnych IDS nad rámec oprávnených účelov.

- Mali by sa navrhnúť špecifické opatrenia na ochranu súkromia, ako je zovšeobecnenie alebo rušenie, ktorými by sa nenarušil celkový obraz o stave prostredia a možnosť identifikovať nové nebezpečenstvo, ale obmedzilo by sa zbytočné vystavenie alebo dlhodobé sledovanie vodiča.
- Osobitná pozornosť by sa mala venovať frekvencii zmeny certifikátov s cieľom vytvoriť spravodlivú rovnováhu medzi zvolenou frekvenciou a rizikami dlhodobého sledovania.
- Osobitné kategórie údajov a údaje súvisiace s odsúdeniami a trestnými činmi by sa nemali vysielať.
- Je potrebné dôkladne posudzovať kvalitu údajov tak, aby sa obmedzilo riziko využívania kooperatívnych IDS, ktoré nie je neutrálne, riziko generovania falošných poplachov alebo naopak nesprávny výklad skutočných núdzových situácií.
- Mechanizmus infraštruktúry verejného kľúča na distribúciu certifikátov by mal byť podrobne verejne zdokumentovaný a prísne monitorovaný, aby sa zamedzilo riziku kolúzie medzi certifikačnými orgánmi a partnermi alebo riziku zásahov aktérov nekonajúcich v dobrom úmysle.
- Je potrebné jasne uviesť obdobie uchovávania spracúvaných údajov všetkými stranami zainteresovanými na platforme kooperatívnych IDS a zakázať vytváranie centralizovanej databázy vymieňaných správ akýmikoľvek subjektmi kooperatívnych IDS.