Műhelytanulmány

# A közös európai mobilitási adattér és az ITS ökoszisztéma tanúsíthatósága

Beküldve: 2021.01.15.
Elfogadva: 2021.06.30.
Online közzétéve: 2022.10.24.

**BÓDI ANTAL** ITS irodavezető, tudományos munkatárs, Közlekedéstudományi Intézet, ITS Tanúsító Iroda, bodi.antal@kti.hu
**DR. MAROS DÓRA** tanúsítási szakértő, tudományos tanácsadó, Közlekedéstudományi Intézet, Vasúti Ellenőrző-, Irányító- és Jelző Iroda (CCS), maros.dora@kti.hu

Absztrakt: A közös európai mobilitási adattér tudatos kialakítása alapvető kiberbiztonsági kérdéseket vet fel. Jelen cikk a 2020-ban elfogadott európai adatstratégiából kiindulva, több szempont (normatív rendeletek, az Európai Bizottság kezdeményezései, kiberbiztonsági tanúsítás, hiányzó feltételek) alapján javaslatokat fogalmaz meg az intelligens közlekedési rendszerek (ITS) ökoszisztémában a közlekedés egészére vonatkozó biztonsági napló kialakítása kapcsán. Hazánk ebben a folyamatban vezető szerepet tölthetne be, ha az eddig elért eredményeket innovatívan és kreatívan hasznosítja az ITS fejlesztésében, beleértve a hálózatba kapcsolt járműveket is. A mobilitási adattér megkönnyíti a hozzáférést a közlekedési és mobilitási adatbázisokból származó adatokhoz, azok összevonását, megosztását és a közhiteles tanúsíthatóságát, kapcsolódva a kialakítás alatt álló európai kiberbiztonsági keretrendszerhez és a zéró bizalom elvéhez.

*Kulcsszavak: európai adatstratégia; mobilitási adattér; 5G; trust space; ITS ökoszisztéma*

## The Common European Mobility Data Space and the certifiability of the ITS ecosystem

Abstract: The conscious development of a common European Mobility Data Space raises fundamental cybersecurity issues. This paper gives a proposal for the development of a transport-wide safety log for the Intelligent Transport Systems (ITS) ecosystem, based on the European Data Strategy 2020, and taking into account several aspects (normative regulations, European Commission initiatives, cybersecurity certification, missing links). Hungary could play a leading role in this process by using the results achieved so far in an innovative and creative way in the development of ITS, including connected vehicles. The Mobility Data Space will facilitate access to, aggregation, sharing and public certification of data from transport and mobility databases, linked to the European cybersecurity framework under development and the principle of zero trust.

*Keywords: European data strategy; mobility data space; 5G; trust space; ITS ecosystem*

## Bevezetés

A kiterjedt digitalizáció lehetősége és igénye a közlekedést is elérte (Ducuing, 2020). Olyan intelligens közlekedési rendszerek (Intelligent Transport Systems, ITS) jönnek létre, amelyek az általuk előállított és kezelt adatokra épülve lehetővé teszik a közlekedési adattér kialakulását (Bódi – Maros, 2019). A lehetőségek kiaknázása azonban jelentős kockázatot is hordoz magában, mivel az ITS kialakítása során fokozott kitettséget és kiberfizikai kockázatot jelentő IT rendszereket vagyunk kénytelenek használni (Sallai et al., 2009; Bódi et al., 2018). Azzal, hogy adatvezérelt hálózati rendszerek közvetlen emberi kontroll nélkül képesek a közlekedésben meghatározó szerepet játszani, a felelősség meghatározásában és a jogkövető magatartás kikényszerítésében, a jogalkotás és a jogértelmezés számára nagyon komoly kihívást jelentenek. A technológiai fejlődés olyan új lehetőségeket ad a kezünkbe, amelyek segítségével képesek leszünk a kialakuló helyzetet kezelni, és a kockázatokat megszüntetni vagy legalábbis jelentősen mérsékelni.

# Európai adatstratégia, mobilitási adattér

Az európai adatstratégia[1] fogalmazza meg, hogy a 21. századi átalakulás középpontjában az adatok állnak. Az adatvezérelt innovációk a polgárok számára óriási előnyöket nyújtanak majd. Például mindeddig csak tudományos-fantasztikus művekben láthattunk példát a személyre szabott orvoslásra, a 2020-as években pedig már távsebészeti beavatkozások elvégzése is rutinszerűvé válhat. Olyan újfajta adatvezérelt mobilitási lehetőségek bontakoznak ki, amelyek az európai zöld megállapodásban kitűzött klímacélok megvalósulását lehetővé teszik majd.

Olyan társadalomban fogunk élni, ahol az egyének egyre több adatot állítanak elő. Az adatgyűjtés és felhasználás módjának elsősorban az egyén érdekeit kell előtérbe helyeznie, összhangban az európai értékekkel, az alapvető jogokkal és a szabályokkal. A felhasználók többségében még nem tudatosult kellőképpen, hogy az adataik nem feltétlenül csak számukra kedvező felhasználásra nyújtanak lehetőséget. Amint negatív tapasztalatokkal találkoznak – például nem kért reklám árasztja el őket, vagy akár nagyon érzékeny egészségügyi adataikat zsaroló vírusok blokkolhatják, ha azok nem megfelelő kezekbe kerülnek –, a társadalom tagjai bizalmatlanná válhatnak. Az állampolgárok csak akkor fognak az adatvezérelt innovációban megbízni, és csak akkor fogadják el azt, ha meggyőződnek, hogy az EU-ban az adatok megosztása során a szigorú uniós adatvédelmi szabályok (GDPR[2]) maradéktalanul érvényesülnek.

A közös európai mobilitási adattér tudatos és tervszerű kialakításánál arra kell hangsúlyozottan törekedni, hogy Európa az intelligens (gépjármű- és egyéb) közlekedési rendszerek kifejlesztésében vezető szerepet töltsön be. Ez az adattér meg fogja könnyíteni a meglévő és a jövőbeli közlekedési és mobilitási adatbázisokból származó adatokhoz való hozzáférést, azok összevonását és megosztását.

Napjainkban a korszerű járművek óránként már mintegy huszonöt gigabájtnyi adatot generálnak, az önvezető autók pedig több terabájtnyi adatot fognak előállítani, amelyeket a mobilitással kapcsolatos innovatív szolgáltatásokhoz, valamint a javítási és a karbantartási szolgáltatásokhoz lehet majd felhasználni. Ezen a területen az innovációhoz szükség van arra, hogy az autók adatait az érdekelt szereplők (stakeholderek) között biztonságosan, jól szervezetten és a versenyszabályokkal összhangban megosszák. A járművek fedélzeti adataihoz való hozzáférést az uniós járműjóváhagyási jogszabályok már 2007 óta szabályozzák, annak érdekében, hogy a független javítóműhelyek számára egyes gépjárműadatokhoz méltányos és kielégítő hozzáférést biztosítsanak. Napjaink változó elvárásaival és a becsült jövőbeli adattömegekkel kapcsolatos jövőbeli elvárásokkal összhangban az említett jogszabályok frissítése folyik – annak érdekében, hogy elősegítsék az összekapcsolt rendszerek terjedését. A távközlésben gyors fejlődésnek lehetünk szemtanúi, amelyek az ún. távdiagnosztikai és felügyeleti rendszerek számára egyre biztonságosabb és egyre nagyobb kapacitást képesek biztosítani. Az 5G-rendszerek kialakítása már világszerte megkezdődött, és több országban a 6G-rendszerek kísérleti fejlesztése is elkezdődött. A távközlés fejlődése és a biztonságos szoftverrendszerek fogják biztosítani az adatokat generáló autótulajdonosok jogainak és érdekeinek tiszteletben tartását és az adatvédelmi szabályok betartását.

## Az Európai Bizottság kezdeményezései

Az európai adatstratégián belül a mobilitási adattér létrejöttéhez a Bizottság felülvizsgálja a gépjárművekre vonatkozó hatályos, uniós típusjóváhagyási jogszabályokat (amelyek jelenleg csak a javítási és karbantartási célú, vezeték nélküli adatmegosztásra összpontosítanak) azzal a céllal, hogy azok hatálya több, a gépjárműadatokon alapuló szolgáltatásra is kiterjedjen. A felülvizsgálat keretében többek között arra keresik a választ, hogy a gépjárműgyártók miként teszik, illetve miként tegyék hozzáférhetővé az adatokat, valamint milyen eljárások szükségesek ahhoz, hogy az ilyen adatok lehívása az adatvédelmi szabályok, valamint a gépjármű-tulajdonosok és a gépjárművezetők jogainak maradéktalan tiszteletben tartása mellett történjen.

Az intelligens közlekedési rendszerekről szóló irányelv és az ahhoz kapcsolódó felhatalmazáson alapuló rendeletek 2010-es évek végén indult felülvizsgálata kapcsán az adatok rendelkezésre állásának, újrafelhasználásának és interoperabilitásának további elősegítésére erősebb koordinációs mechanizmust hoznak létre. Ennek célja, hogy az Európai Hálózatfinanszírozási Eszköz (CEF) támogatásával és annak keretében az ITS-irányelv[3] alapján

[1] A Bizottság közleménye: Európai adatstratégia, COM(2020) 66, 2020. február 19.
[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), 2016. április 27.

létrehozott nemzeti hozzáférési pontokat egyesítse és egységesítse.

2020-ban módosították az egységes európai égboltról szóló rendeletre irányuló javaslatot[4], új rendelkezésekkel bővítve azt az adatok rendelkezésre állására és az adatszolgáltatók piaci hozzáférésére vonatkozóan, annak érdekében, hogy a légi forgalmi szolgáltatás digitalizálását és automatizálását előmozdítsák. Ennek köszönhetően a légi közlekedés biztonsága, hatékonysága és kapacitása a remények szerint jelentősen javul. A drónok működését szabályozó rendeleteket például a jövőben nemzeti szinten is kiadják (Beke et al., 2018). Ezenkívül a vasúti közlekedés területén alkalmazott interoperábilis adatmegosztásra vonatkozó szabályozási kereteket is felülvizsgálják 2022-ig. Az elektronikus árufuvarozási információkról szóló rendeletekben előírt közös adatkészleteket azzal a céllal hozzák létre, hogy a vállalkozások és a közigazgatási szervek közötti digitális adatcserét, az adatok újrafelhasználását és az adatok másodlagos felhasználását megkönnyítsék.

## Kiberbiztonsági tanúsítás

A Bizottság felismerte, hogy az informatikai kitettség kezelésére fokozott figyelmet kell fordítani. Az EU rendeletben[5] megbízta az ENISA-t (az Európai Uniós Kiberbiztonsági Ügynökséget), hogy dolgozza ki az információs és kommunikációs technológiák kiberbiztonsági tanúsításának eljárását, mivel a hálózati és az információs rendszerek, valamint a távközlési hálózatok és szolgáltatások a társadalom működésében létfontosságú szerepet töltenek be, és a gazdasági növekedés gerincét képezik. Ezt az irányelvet 2025. június 28-ától a közlekedési szolgáltatásokra is alkalmazni kell. Ez kiterjed a légi, a vasúti, a vízi és az autóbusszal végzett személyszállítási szolgáltatások alábbi elemeire (a városi, az elővárosi és a regionális közlekedési szolgáltatások kivételével, amelyeknél csak az v. alpont szerinti elemeket kell alkalmazni):

i. honlapok;
ii. mobileszköz-alapú szolgáltatások, ideértve a mobilalkalmazásokat is;
iii. elektronikus menetjegyek és elektronikus menetjegy-értékesítési szolgáltatások;
iv. a személyszállítási szolgáltatásokkal kapcsolatos tájékoztatás, a valós idejű utazási információkat is beleértve; ez az információs képernyők tekintetében az EU területén található, interaktív képernyőkre korlátozódik;
v. az EU területén található interaktív önkiszolgáló terminálok, kivéve azokat a járműveket, repülőgépeket, hajókat és vasúti járműveket, amelyekbe beépítették már korábban ezeket a terminálokat.

Ebben a felsorolásban nem találkozunk sem adatstratégiával, sem mobilitási adattérrel, annak ellenére, hogy ennek a kialakítására szabott határidő sokkal későbbi, mint a mobilitási adattér kialakíthatóságához kapcsolódó intézkedéseké – és ez minden bizonnyal konfliktushoz fog vezetni és utólagos harmonizációt fog igényelni.

## Normatív rendeletek

A már említett GDPR a természetes személyek személyes adatainak a kezeléséről és azok védelméről szól, általában ezt tekintik az általános adatvédelmi rendeletnek. Ez az európai jogintézmény az adatvédelem fontosságára nem csak az EU-tagországok állampolgárait ébresztette rá, hanem az egész világ számára mintaként szolgál(hat).

Az eIDAS[6], az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendelet minden tagországra vonatkozó szabványosítási előírás, amely az elektronikus azonosítók és aláírások elfogadására konzisztens jogi kereteket biztosít. Az üzleti egységek számára digitális pecséteket is bevezet, és így az eIDAS megérkezésével az európai szervezetek üzleti folyamatainak teljes digitalizálása válik lehetővé, azonban ezt 2020-ig nem sikerült minden tagországban egyenlő szinten bevezetni. Magyarország ezen a területen élen jár, mivel az e-személyi igazolvány eIDAS-konform eszköz, és már a magyar lakosság mintegy fele rendelkezik is ilyen eszközzel. Az eIDAS rendelet jelenleg módosítás alatt áll, annak érdekében, hogy az eltérő nemzeti szintű megoldásokat egységes uniós rendszer váltsa ki egységes, elektronikus személyazonosítási rendszer létrehozásával. A jelen tanulmány írásakor fennálló koronavírus-világjárvány kezelése felgyorsíthatja ezt a folyamatot, amennyiben a rendelet a jelenlegi PASS funkció mellé „víruspassport” funkcióval is kiegészül majd.

[3]Az Európai Parlament és a Tanács 2010/40/EU irányelve az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről, 2010. július 7.
[4]Az Európai Parlament és a Tanács rendelete az egységes európai égbolt végrehajtásáról (átdolgozás), COM(2020) 579, 2020. szeptember 22.
[5]Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), 2019. április 17.
[6]Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről, 2014. július 23.

A NIS[7] direktíva az EU 2016/1148 irányelve, amely a hálózati és az információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedések kidolgozását irányozza elő. Ennek a reformja is tervbe van véve, és a NIS2 kialakításáról napjainkban széles körű egyeztetés van folyamatban.

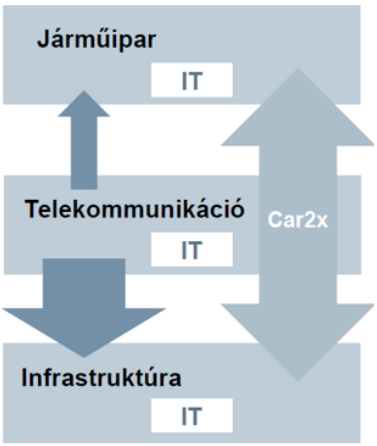
A fenti három rendelet által meghatározott jogszabályi környezet jelentős támogatást ad a mobilitási adattér létrejöttének a megalapozásához.

### Hiányzó feltételek

Egyes fejlesztőlaborokban már jelentős eredmények születtek a jövő közlekedését érintően. Az 1. ábra bemutatja, hogy a fő együttműködő partnerek – járműgyártás, infrastruktúra-fejlesztés, távközlési szolgáltatás – között milyen kapcsolódás, együttműködés, azaz logikai modell képzelhető el. A legnagyobb problémát az okozza, hogy ebben a struktúrában az alábbi szerepeket még nem dolgozták ki:

- Hatósági, állami szerepek definiálása;
- Bűnüldözés, bűnmegelőzés, terrorelhárítás feltételrendszere;
- Az egész ITS ökoszisztémát tanúsító szervezetek szerepe és lehetősége;
- A garanciát, illetve a biztosítást nyújtó szereplők csatlakozási felülete;
- A különböző típusú járművek heterogén életkorának és felszereltségének a kezelése.

**1. ábra.** A jövő közlekedésében leginkább érintett iparágak együttműködése




Forrás: Üveges – Bogárdi (2019: 5)

## ITS ökoszisztéma – mint biztonsági napló a közlekedés egészére

Az ITS a közlekedésben alkalmazott infokommunikációs technológiák alkotta egységes rendszert jelenti, amelynek segítségével a közlekedési módok mind társadalmi, mind egyéni szempontból optimalizálhatók, azaz javítható a költséghatékonyság, csökkenthető a környezeti terhelés, valamint javítható a közlekedés biztonsága, informáltsága és kényelme. Fejlesztése során a hangsúlyt arra kell helyezni, hogy egyszerre teljesüljenek mind a társadalmi, mind az egyéni szempontok. Ennek alapján az a felvetésünk, hogy az ITS adatokra épülő ökoszisztémát a közhitelesen rögzített közlekedési adatokra támaszkodva kell létrehozni. Ezzel biztosítható a közlekedés egészére az úgynevezett megmásíthatatlan biztonsági napló (security log). Ez esetünkben azt jelenti, hogy a közlekedési trajektóriákat (a közlekedést jellemző pályát, sebességet és időt rögzítő adatokat), és ezzel a közlekedési tér mozgó vagy nem mozgó résztvevőinek állapotváltozását digitálisan és közhitelesen rögzítik. Ennek eredményeként az feltételezhető, hogy a közlekedésben részt vevők viselkedése kedvezően fog változni, mert minden közlekedési aktivitás mérhető és dokumentálható lesz, és ezáltal a közlekedésből származó társadalmi veszteség a jövőben jelentős mértékben csökken, a közlekedésbiztonság pedig érdemlegesen javul. Ezzel a közlekedés egésze – a vonatkozó európai és hazai szabályokkal összhangban – közhitelesen tanúsíthatóvá válik. A gyakorlati megvalósításához

[7]Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, 2016. július 6.

a már elterjedt, flottakövető rendszerekhez hasonló integrált digitális rendszert kell majd kialakítani, amely hatósági rendszerként működik és adatvédelmi szempontból az EU kiberbiztonsági tanúsítása szerint az EU GDPR, valamint az eIDAS és a NIS kötelező érvényű rendeleteinek is megfelelne.

Az előzőek alapján egy bizalmi modell jönne létre, azaz olyan speciális adattér, amely elemeinek kiberbiztonsági védelme garantált és tanúsított (trust space). Az adattérben lévő adatok megmásíthatatlanok, megőrzöttek, kompromittálhatatlanok, adott felhasználásra/felhasználási célra érvényesek és elérhetők. A felhasználás ellenőrizhetőségének mind technikailag, mind pedig törvényi szabályozás szerint a teljes életciklus alatt biztosítva kell lennie. Ez a modell a bizalom két szintjén alapul:

- egyéni szintű bizalom: a szereplők tevékenységének a teljes körű biztonsági logolása;
- rendszerszintű bizalom: a rendszer egészén belüli zéró bizalom (Zero Trust) elvére épül, és ki kell zárni minden olyan elemet, amelynek biztosítása egyéni hozzáálláson vagy ki nem kényszeríthető szabálykövetésen múlhatna.

A fentiekből következően az ITS ökoszisztémát a teljes mobilitási adattér speciális részhalmazaként értelmezhetjük, mint a közlekedés biztonsági naplóját. Ennek kialakítása elő tudja segíteni az autonóm közlekedés kialakulását és a korábban felsorolt hiányzó feltételek megalapozását azzal, hogy minden szereplőről képes lesz közhiteles mobilitási adatokat összegyűjteni. Az ITS ökoszisztéma nem szükségképpen igényel nagy sávszélességű, magas rendelkezésre állású, kiemelt biztonsági paraméterekkel rendelkező hálózati lefedettséget, mint amilyen például az 5G hálózat. Az autonóm közlekedés nagyon nagy adatigényének a kielégítéséhez azonban az 5G képességei elengedhetetlenek.

## Összefoglaló gondolatok

A közös európai mobilitási adattér és az ITS közlekedési rendszerek esetén a kiberfenyegetettség minimalizálása, illetve lehetőség szerinti kizárása kiemelt feladat. Ennek érdekében olyan 5G hálózati lefedettséget kell kialakítani, amely magas rendelkezésre állással és megfelelő biztonsággal képes az adatátvitelre. Az adatok összegyűjtése és mozgatása során az adattér számára részben az 5G hálózat fogja az itt megosztott adatokból létrejövő trust space garantálását és az EU kiberbiztonsági keretrendszer szerinti tanúsíthatóságát is megteremteni. Az ITS ökoszisztéma esetén a közhitelességi és a GDPR elvárások teljesülését rendszerszinten kell garantálni. Ehhez az eIDAS szerint kell kialakítani a hozzárendelhetőséget az eID-hez (elektronikus azonosítóhoz).

További feladat, hogy a jövőben kiberbiztonsági szempontból meg kell vizsgálni a már kialakult forgalomirányító, közlekedésbiztonságot támogató rendszereket, illetve a járműveken belüli, aktív közlekedésbiztonsági rendszerek esetén a mesterséges intelligencia alkalmazhatóságát. Az örökölt (legacy) rendszerek integrálása a közös mobilitási adattérbe kiemelt kiberbiztonsági kockázati tényezőt jelent.

Külön vizsgálatra érdemes a közösségimédia-alapú navigációs rendszerek és a közforgalmú közlekedési rendszerek között megteremthető kölcsönhatás és ezek együttes hatása az adatvezérelt közlekedési rendszerek kialakítására. A közlekedési rendszerekben használt informatikai rendszerek átlagos felhasználóin kívül kiemelten kell kezelni elsősorban a privilegizált felhasználók, a rendszergazdák és az adatgazdák kiberbiztonsági tudatosságát, valamint a szabályok betartását és betartatását, mert az adatbiztonsági sérülékenységek és azok kihasználhatósága a legtöbb esetben emberi hibákra vagy mulasztásokra vezethető vissza.

## Felhasznált irodalom

Beke Éva et al. (2018): The role of drones in linking industry 4.0 and ITS Ecosystems, IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI 2018), IEEE Hungary Section, Budapest, 2018. november 21-22., 191–198. https://doi.org/10.1109/CINTI.2018.8928239

Bódi Antal et al. (2018): ITS ökoszisztéma – A közlekedés egészének digitalizációja, in: Munkácsy András – Jászberényi Melinda (szerk.): Utazás a tudományban. Konferencia a 70 éves Pálfalvi József tiszteletére, Budapesti Corvinus Egyetem, Budapest, 2018. február 23., 82–84. http://unipub.lib.uni-corvinus.hu/3782/1/UaT2018_kotet_vegleges.pdf

Bódi Antal – Maros Dóra (2019): A komplex ITS ökoszisztéma alapjai, in: Vigh László (szerk.): Az infrastruktúra és a gazdaság távlatai 2020 előtt, Acta Periodica 17. kötet, Edutus Egyetem, Budapest, 48–70.

Ducuing, Charlotte: Beyond the Data Flow Paradigm: Governing Data Requires to Look Beyond Data, Technology and Regulation, 2020, 57–64. https://doi.org/10.26116/techreg.2020.006

Sallai Gyula et al. (2009): A hazai szélessávú infokommunikációs infrastruktúra fejlesztése, Híradástechnika LXIV:1-2, 4–17., https://hiradastechnika.hu/data/upload/file/2009/2009_1_2/HT09_1_2a3.pdf

Üveges Péter – Bogárdi Péter (2019): Önvezető és vezetést támogató technológiák közúti infrastruktúrája. Közlekedési Kultúra Napja – Siemens megoldások az autonóm közlekedésben, Budapest, 2019. május 17. https://docplayer.hu/156287023-Onvezeto-es-vezetesttamogato-technologiak-kozuti-infrastrukturaja-siemens-mobility.html

Valamennyi online forrás esetében az utolsó hozzáférés ideje: 2020. december 17.