THE REGULATORY LANDSCAPE FOR MOBILITY AS A SERVICE IN A EUROPE FIT FOR THE DIGITAL AGE

František Kasl / Pavel Loutocký / Adam Jareš /
Veronika Příbaň Žolnerčíková / Martin Erlebach

František Kasl, Ph.D., postdoctoral researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Veveří 158/70, 611 80 Brno, CZ, e-mail: frantisek.kasl@muni.cz

Pavel Loutocký, Ph.D., postdoctoral researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Veveří 158/70, 611 80 Brno, CZ, e-mail: loutocky@muni.cz

Adam Jareš, Ph.D., postdoctoral researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Veveří 158/70, 611 80 Brno, CZ, e-mail: 518466@muni.cz

Veronika Příbaň Žolnerčíková, researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Veveří 158/70, 611 80 Brno, CZ, e-mail: 477105@muni.cz

Martin Erlebach, junior researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Veveří 158/70, 611 80 Brno, CZ, e-mail: 480066@muni.cz

Keywords: ***mobility as a service, digitalisation, data governance, cybersecurity, data act, data governance act, digital markets act, digital services act, NIS2 directive***

Abstract: *The digitalisation is transforming all aspects of modern society; it also brings new models and services to urban mobility. Mobility as a service represents such new services based on shared mobility enabled by data driven coordination and optimisation. The new regulatory frameworks on data governance implementing the EU strategy for the digital transformation are currently in final stages of adoption. In our contribution, we seek to provide a timely reflection of the opportunities and limits that are to be set by these legislative acts on the future of mobility as a service in the EU.*

1. Introduction[1]

Modern mobility indicates a growing shift towards digitalised transport, which combined with platform business models enables new approaches to efficient and sustainable modes of transportation. *Mobility as a service* (MaaS) is conceptual characterisation of this shift build upon availability of data collection, processing and communication capabilities that offer a bridge between total dependence on public transport and unsustainable social as well as individual burdens of mass vehicle ownership. The shift to on demand, coordinated, shared and optimised transport service promise to combine benefits of individual mode of transport with efficient use of space, resources and capacities of the transport infrastructure. "*The desire to adopt MaaS as a solution is now widely supported, and will depend on the notion that urban mobility must rapidly become fully*

[1] This article was created on the basis of the project support of the Technology Agency of the Czech Republic within the project "*Ochrana datových toků ve sdílených dopravních prostředcích*" [Protection of data flows in shared means of transport] with the identification code CK03000040.

multifaceted, to minimise the negative impact of increased external costs."[2] The growing practical experience with various business models that fit into the concept of MaaS indicate that there are growing opportunities for such element in the modern multi-modal mobility landscape, but also that it needs to be suitably fitted into the particular setting of the given municipal environment and often actively interconnected with the network of public transport to reach full benefits and bring maximal contribution to cost-efficient mobility solutions.

The EU is pursuing innovation and improvement of the mobility landscape on a number of levels, with close link between the modernised transport system and goals of sustainable zero-emission economy envisioned under climate and energy strategies liked to the Commission´s priority known as the *European Green Deal*.[3] There is a number of policy and regulatory initiatives build into the broader shift in approach to transport in EU,[4] but probably the most relevant are measures pursued under the new European urban mobility framework.[5] MaaS is closely intertwined with these measures, as suitable development of efficient market environment in transport services that provide e.g. the last mile transport in lower traffic density areas will allow better optimised public transport planning, while achieving the decrease in overall individual traffic and retained mobility options and comfort for the passengers in question. As a data-driven commercial solution, the MaaS business models need to align with the appropriate regulatory requirements, in particular concerning the data processing and sharing. "*For the digital revolution to be fully exploited, MaaS must be considered as a way of managing the common good – public space – through the creation of another common good; a public data platform.*"[6]

In this regard, the whole European regulatory landscape is currently undergoing a major change that will set the foundation of future digitalised economy. This is linked to another of the strategic priorities of the European Commission, in this case known under the title *A Europe fit for the digital age.*[7] This digital strategy is set to strengthen digital sovereignty of the EU and set world-leading standards for data processing, sharing and re-use. It is aimed at the development of a data-agile economy and covers a number of new regulatory initiatives.

In our contribution, we aim to focus on four areas in particular:

(1) the establishing of a cross-sectoral governance framework for data access and use, represented by the new Data Governance Act (DGA)[8] provisions on data-sharing as well as the development of the *Common European Mobility Data Space* for sectoral data sharing and data pooling;[9]

(2) the new framework aimed at empowering individuals to control their data within the new data-sharing architecture and governance mechanisms, as foreseen in the proposed Data Act (DA);[10]

---

2 Cf. Cerre, Mobility as a Service (MaaS): A digital roadmap for public transport authorities. https://cerre.eu/publications/mobility-as-a-service-maas-digital-roadmap-public-transport-authorities/ (accessed on 23 December 2022), 2021, p. 13.

3 Cf. European Commission, A European Green Deal. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en (accessed on 23 December 2022).

4 Cf. European Commission, New transport proposals target greater efficiency and more sustainable travel. https://transport.ec.europa.eu/news/efficient-and-green-mobility-2021-12-14_en (accessed on 23 December 2022), 2021.

5 Ibid.

6 Cf. Cerre, Mobility as a Service (MaaS): A digital roadmap for public transport authorities. https://cerre.eu/publications/mobility-as-a-service-maas-digital-roadmap-public-transport-authorities/ (accessed on 23 December 2022), 2021, p. 51.

7 Cf. European Commission, A Europe fit for the digital age. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (accessed on 23 December 2022).

8 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868 (accessed on 23 December 2022).

9 Cf. European Commission, Workshop on a Common European Mobility Data Space. https://digital-strategy.ec.europa.eu/en/events/workshop-common-european-mobility-data-space (accessed on 23 December 2022), 2021.

10 Proposal for a Regulation (EU) on harmonised rules on fair access to and use of data (Data Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN (accessed on 23 December 2022).

(3) transformation of competition and liability rules reflecting the shift in the digital economy landscape and ensuring fair competition of all companies, as set in the Digital Markets Act (DMA)[11] and Digital Services Act (DSA)[12]; and

(4) new cybersecurity rules and requirements applicable to broader spectrum of sectors including the MaaS and digitalised mobility solutions, as set in particular in the proposal of NIS 2 Directive.[13]

We will highlight the relevance of these new regulatory frameworks for the MaaS concept and discuss the opportunities and limitations for realisation of MaaS solutions in light of these new provisions.

2. Data Governance Act

The EU recognises the transformation of the economy driven by digital technologies and that data is at the core of this development. Further development should therefore be based on data that may contribute, among other things, to new possibilities in mobility. European Commission therefore proposed the establishment of common European data spaces for data sharing and data pooling. These common European data spaces should also cover the area of mobility.[14]

The Data Governance Act (DGA), which was adopted on 30 May 2022 and shall apply from 24 September 2023, lays down conditions for the re-use of certain categories of data[15] held by public sector bodies.[16] For the purposes of DGA "re-use" is defined as the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced.

It is necessary to mention that DGA does not create obligation of public sector bodies to allow the re-use of data. However, DGA prohibits agreements or other practises pertaining to the re-use of specified data which lead to exclusive rights to data or to a restriction of availability of such data for re-use by other entities. The only exception is in situations where without an exclusive right to re-use data the provision of a service or the supply of a product in the general interest would not otherwise be possible.[17]

Although DGA does not explicitly regulate the area of MaaS and data generated by MaaS, it will impact MaaS in the area of re-use of such data. While public sector data holders will not be obliged to allow the re-use of data under DGA, on the other hand, they are, with the exceptions mentioned above, prohibited from establishing exclusive agreements and using other practices that would restrict the re-use of data by other entities. If a public sector holder of data generated by the operation of MaaS were to impose any conditions on the re-use of that data, those conditions must be non-discriminatory, transparent, proportionate and objectively justified with regard to the MaaS data. At the same time, these conditions must not be used to restrict business competition.

---

[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925 (accessed on 23 December 2022).

[12] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065 (accessed on 23 December 2022).

[13] Proposal for a Directive (EU) on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823 (accessed on 23 December 2022).

[14] Recital 2 of DGA.

[15] The main scope are data held by public sector bodies which are protected on grounds of commercial confidentiality, including business, professional and company secrets, statistical confidentiality, the protection of intellectual property rights of third parties, the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024 on open data and the re-use of public sector information. Cf. Article 3 DGA.

[16] Article 1 para 1 DGA.

[17] Article 4 para 1 and 2 DGA.

Another objective of DGA is to support so-called data altruism. This term introduced by DGA means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data. The idea behind it is that such data subjects or data holders will share their personal or non-personal data without seeking or receiving a reward[18] for objectives of general interest, improving the provision of public services, public policy making or scientific research purposes. As one of these areas DGA specifically mentions is the improvement of mobility.[19] It is possible to imagine that some MaaS users will be willing to voluntarily share their data generated by using MaaS through data altruism organisations.

We believe that re-use of data generated by vehicles used for private or public transportation could foster innovation and further development of MaaS. Such data may also contribute to data driven planning policies, urban planning and zoning.[20] It is therefore crucial to provide conditions for a broad re-use of data generated by intelligent transport systems and vehicles. On the other hand, it is also necessary to maintain the security of data and the rights of data subjects or data holders. In this context, it is necessary to take into account that the DGA is only a general regulation[21] and its implications for MaaS are likely to be modified by sector-specific regulation. DGA directly foresees this by stating that *"[s]ector-specific Union law can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the Union law envisaged on the European health data space and on access to vehicle data."*[22] DGA therefore lays down only general rules for the re-use of data which includes data generated by vehicles and other devices used for MaaS and promotes such re-use in general. Thus, in further considerations of re-use of data generated by MaaS, it is necessary to take into account other relevant European legislation, in particular in the field of data protection,[23] cyber security or forthcoming sector-specific regulation.

3. Data Act

The Data Act (DA) was proposed by the European Commission in February 2022 and is currently undergoing standard legislative procedure, with no definite timeframe of adoption.[24] Nevertheless, it is a crucial piece of the new regulatory landscape of European digital economy. While DGA creates the processes and structures to facilitate data re-use, DA shall clarify who can create value from data and under which conditions. This makes DA horizontal proposal setting basic rules for all sectors with an impact similar to the adoption of GDPR. It should foster business-to-government data sharing for the public interest and support business-to-business data sharing. It is expected to facilitate access to and use of data by consumers while preserving incentives to invest in ways of generating value through data.

It presents measures to allow users of connected devices to gain access to data generated by them and to share such data with third parties to provide aftermarket or other data-driven innovative services, measures to prevent abuse of contractual imbalances in data sharing contracts and reinforced data portability right. It should lead to fairer and more balanced data sharing contracts of SMEs with dominant companies.

---

18 Except for compensation that goes beyond compensation related to the costs that they incur where they make their data available.

19 Article 16 para 16 DGA.

20 Cf. Mouratidis/Peters/van Wee, Transportation technologies, sharing economy, and teleactivities: Implications for built environment and travel, *Transportation Research Part D: Transport and Environment*, Amsterdam: Elsevier, Volume 92, 2021, ISSN 1361-9209, https://doi.org/10.1016/j.trd.2021.102716, pp. 2 and 17.

21 Cf. Article 1 para 2 DGA.

22 Recital 3 DGA.

23 For implications of intelligent transport systems on data protection of personal data see Article 29 Data Protection Working Party. Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS). http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888 (accessed on 23 December 2022), 2017.

24 Cf. European Parliament, The Data act: Briefing. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733681 (accessed on 23 December 2022), 2022.

In several aspects offers the DA rather challenging future settings for numerous currently pursued digital economy models, in particular sharing economy concepts. There are several interesting moments in connection to MaaS deployment. Articles 3 and 4 DA of the proposal foresee access of the user to the data (personal as well as non-personal) generated by use of the service. It may be an obligation with a positive impact, opening the data processing in MaaS to greater scrutiny and allowing innovation by accessibility of the data for further use based on Article 5 DA. Nevertheless, not only for MaaS, the interpretation and in particular enforcement of this right will greatly define it resulting effect. The accessibility is conditioned by a set of exceptions and limitations that may rest on protection of personal data, scope of trade secrets, interpretation of link between data generation and use (ie. is data generated by the engine sensors during the usage of the leased car data generated by the user in the meaning of DA?). Additionally, the small and micro enterprises are exempt from these obligations, which may lead to purposeful fragmentation and obfuscated chaining of business entities to avoid these obligations or to take maximal advantage of the possible access to these data generated by other entities on the basis of Article 5 DA. The Council is set to discuss the proposal on 6 December 2022, which may lead to major amendments of the proposal or expose the lack of consensus that may delay the adoption of the act significantly (similar to for example the still not adopted e-Privacy Regulation[25]).

Beyond regulating the conditions for data holder granting access to generated data to third party and streamlining of rules for unfair terms in such set up, DA further set conditions for mandatory grant of access to public sector bodies based on exceptional need scenarios, as regulated in proposed Articles 14–22 DA. Nevertheless, pursuant to the definition of exceptional need to use data in Article 15 DA, we conclude that MaaS are unlikely to be affected by this obligation. Similarly, the requirements designed for effective switching between providers of data processing services under Article 23–26 DA should not pose particular challenges to MaaS providers, as the data generated by their use are largely bound to the technical specification of the vehicles, but depending on interpretation of the breath of commercial, technical, contractual and organisational obstacles targeted in Article 23 para. 1 DA, the gamification aspects of MaaS may need to be reconceptualized and some of the options for achieving a sustainable business model in MaaS through user pool stability will likely not be viable under DA.

The structured call for systematically pursued interoperability under Articles 28–30 DA may be to great benefit of MaaS, as common data structures, taxonomies, interfaces or even smart contract standards would significantly streamline the current diverse landscape of MaaS initiatives and should allow greater synergies, including functional connection of MaaS to municipal public transport in a cohesive public-private urban transport system.

DA and DGA aim at enhancing data sharing and reuse of data, while safeguarding the privacy and data protection rights of EU citizens, but this goal remains challenging, as it will likely create inconsistencies and clashes between provisions, which will make guidelines and enforcement key in achieving the functional balance. This will also require finding a reliable way to differentiate personal and non-personal data subject to DA and DGA, in order to align the approach to data as a common pool-resource that should be broadly accessed and used with the rights and expectations of data subjects.

The goal to protect the privacy and safety of EU citizens is further challenged when AI is involved in the operation. This area is covered by the AI Act.[26] The AI Act imposes obligations on so-called high-risk AI systems. According to the proposed legislation, most AI operating in the road traffic environment is considered to be high-risk. Whether it is a component of a physical product or a stand-alone software. However, motor

[25] Proposal for a Regulation (EU) concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 (accessed on 23 December 2022).

[26] Proposal for a Regulation (EU) laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (accessed on 23 December 2022).

vehicles are excluded[27] from the application of the AI Act.[28] AI systems operating in road traffic shall be regulated separately by new legislation. Nevertheless, the new legislation must uphold the level of safety set by the AI Act. On the other hand, AI systems serving as safety components in the management or operation of road traffic are also considered to be high-risk and fall under the scope of the AI Act.

4. DMA & DSA

The spread of MaaS is closely linked with the online platforms and apps aggregating multiple transport modes into themselves.[29] This provides great convenience for consumers, but it is also a regulatory challenge. Digital Markets Act (DMA) is currently in the process of adoption by the EU, while Digital Services Act (DSA) was already adopted. These frameworks for digital economy focus on regulating the intermediary platforms and technological companies with a broad user base identified as "gatekeepers".[30]

There are two layers to this approach. The first one concerns the current state of the MaaS adoption process. There are currently very few international companies providing MaaS services active in the EU.[31] As such, DMA application on MaaS currently remains largely hypothetical, unless one of the already established big tech companies (eg. Alphabet)[32] starts providing MaaS. In this case a plethora of new obligation arises to the platform, such as the ban on treating its own services more favourably in ranking them.[33] This could be the case if own MaaS were recommended or treated advantageously in eg. search or map services. An interesting obligation from the DSA is the need to disclose in the terms and conditions "*the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters."*[34] If provided by a very large online platform, it must also include an option of a service not based on profiling, which may significantly distort the benefits derived from the MaaS in question by the user.[35]

MaaS platforms are likely to meet all three levels of intermediary services under Article 3 lit g) DSA. This means that current MaaS platforms or apps will need to focus on dealing with the risk of illegal content being uploaded to the platform by users, be it consumers or business users. This is then coupled with the need to disclose in the terms and conditions how monitoring of content uploaded by users is done.[36]

5. NIS 2

The final considered area of upcoming EU digital economy regulation that shall be reflected in this contribution concerns cybersecurity, particularly the perspective of proposed NIS 2 Directive.

This revision builds on the original NIS Directive[37], which broadly sets out the obligations relevant in our context, in particular for operators of intelligent transport systems[38], which are the *„systems in which infor-*

27 This statement applies to all legislation enlisted in Annex II, Section B of the AI Act.

28 Apart from two provisions: a) regulatory sandboxes (Art. 53 AI Act) and b) evaluations and reviews of AI Act (Art. 48 AI Act).

29 Cf. Pita, MaaS Alliance position paper concerning the proposed Digital Services Act Package. https://maas-alliance.eu/wp-content/uploads/sites/7/2021/02/MaaS_Alliance_DSA_Final070920.pdf (accessed on 23 December 2022), 2021, p. 1.

30 Article 3 of DMA.

31 Cf. Pita, MaaS Alliance position paper concerning the proposed Digital Services Act Package. https://maas-alliance.eu/wp-content/uploads/sites/7/2021/02/MaaS_Alliance_DSA_Final070920.pdf (accessed on 23 December 2022), 2021, p. 3–4.

32 By this we mean the already established tech giants such as Microsoft, Alphabet or Amazon.

33 Article 6 lit d) of DMA.

34 Article 27 of DSA.

35 Article 38 of DSA.

36 Article 14 of DSA.

37 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32016L1148 (accessed on 23 December 2022).

38 Attachment II, point 2 lit d) NIS Directive.

mation and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport"[39]. Such operators can be considered as operators of an essential service, if they fulfil the additional determining criteria set out in Article 5 para. 2 of the NIS Directive (thus, not every operator of intelligent transport systems can be considered as an operator of an essential service, which is then subject to the conditions set out in the NIS Directive).[40] If operators are considered to be operators of an essential service, they are primarily subject to the obligations set out in Articles 14 and 15 of the NIS Directive. In brief, these include the obligation to prevent and the need to minimise the impact of incidents and attacks, the need to take appropriate technical and organisational measures to manage security risks, to prevent incidents affecting network security and, in the event of a serious impact, to report incidents to the competent authority or CSIRT.

Although the NIS 2 Directive is still undergoing the legislative process, its pre-final wording indicates that the range of obliged entities relevant in the context of MaaS will remain similar.[41] However, under the NIS 2 Directive, the designation of obliged entities and the related obligations are changing. ITS operators are likely to be referred to as essential entities (rather than essential services as they were established under the NIS Directive) and will be considered as any entity listed in Annex I to the NIS 2 Directive. Thus, there will be a move away from the limited designation of obliged entities based on determining criteria, and any ITS provider should be an essential entity under the NIS 2 Directive.[42]

The NIS 2 Directive clarifies the obligations and impacts for the essential entities compared to the previous legislation and sets new specific obligations for the entities concerned. The main purpose, in addition to increasing the level of security of individual obliged entities and covering a more comprehensive range of obliged entities, is also to strengthen the role of the European Network and Information Security Agency (ENISA) in terms of collecting and circulating relevant information (also by operating a European Vulnerability Register)[43] or to introduce cross-border sharing of information on cyber security in general.[44]

Essential entities must specifically develop and adopt more detailed technical and organisational measures to manage security risks, including developing a cybersecurity strategy.[45] They have more obligations related to the reporting of significant incidents[46] (this means significantly broader coverage of incidents than in the case of the NIS Directive and the obligations defined here for reporting incidents with a severe impact) and a reduction of the reporting time to 24 hours (however, with the possibility to deviate from this limit upon agreement with the competent authority)[47]. In addition, under the NIS 2 Directive, the supervision and enforcement of the obligations under introduced legal regime, particularly of essential entities, are also intensified compared to the previous regulation.[48]

---

39 Article 4 para. 1 Directive (EU) 2010/40 of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010L0040&qid=1672147854997 (accessed on 23 December 2022).

40 These criteria are according to Article 5 para. 2 of the NIS Directive as follows: „*(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service*."

41 See Annex I, point 2 letter d) of the NIS 2 Directive.

42 This is similarly to the NIS Directive defined under Article 4 para. 1 of the Directive (EU) 2010/40.

43 Article 6 NIS 2 Directive.

44 Article 26 NIS 2 Directive.

45 See a more detailed overview in Article 18 para. 2 NIS 2 Directive.

46 Article 20 NIS 2 Directive.

47 Article 20 para. 4 NIS 2 Directive.

48 Article 29 or 31 NIS 2 Directive.

The NIS 2 Directive then foresees the possibility of using certification schemes[49] *inter alia* for MaaS related technologies, according to the basic requirements set out in the Cybersecurity Act.[50] Still, it should be noted that, to the date, the individual certification schemes have not yet been approved and the specific implications are thus currently unclear. Additionally, ENISA presented guidelines on implementing the NIS Directive towards the issue of „smart" cars,[51] specifically in cybersecurity related to the automated driving environment.[52] Given the interconnectedness with the MaaS issue, it is then appropriate to reflect such a background, especially in the context of the NIS 2 Directive.

Additionally, the Directive on resilience of critical entities (RCE Directive)[53] is a brand-new legislation, and it complements the changes proposed under NIS 2 Directive. The RCE Directive reflects the increasing synergy between the physical and digital world and aims to mitigate the risks that critical entities face. These risks are identified in multiple areas, two of which concern MaaS. Firstly, the RCE Directive identifies the risk in sectors where operators are reliant on each other and disruption affecting one of them can create a cascading effect. Secondly, the RCE Directive mentions unmanned vehicles as one of the challenges to the environment where critical entities operate.[54] According to Article 5 of the RCE Directive, it is expected that the critical entities under the RCE Directive and the critical infrastructure according to the NIS2 Directive will overlap. Furthermore, unmanned vehicles and other AI systems that are intended to be used as safety components in the management and operation of critical digital infrastructure are considered to be high-risk AI systems according to the AI Act.[55] Notably, the term critical digital infrastructure shall be interpreted according to the RCE Directive.

6. Conclusion

In this contribution, our aim was to provide an analysis of the set of recently or currently adopted components of the new EU legislative framework for digital economy, in particular DGA, DA, DMA, DSA and NIS 2 Directive with the focus on likely opportunities and limits ensuing for MaaS. All these legislative acts have potential to impact the approach to MaaS, although none provides a specific and focused regulation of MaaS *per se*. The limits will mostly concern additional information and data security requirements, even though data access and re-use may also influence the approach to future MaaS. Nevertheless, the new frameworks should be mainly seen as opportunities for better conditions for development and expansion of MaaS, contributing to better interoperability, more resilient and reliant services and better access to data currently out of reach by other data holders. At any rate, MaaS would benefit from further regulatory guidance and service-specific regulation, both bridging the increasingly complex and intertwined regulatory landscape.

49 Article 21 NIS 2 Directive.

50 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 (Cybersecurity Act). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881 (accessed on 23 December 2022).

51 Cf. ENISA, ENISA good practices for security of Smart Cars. https://www.enisa.europa.eu/publications/smart-cars (accessed on 23 December 2022), 2019.

52 For an overview of the available recommendations and reports, see Benyahya/Collen/Kechagia/Nijdam. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments, *Computers & Security*, Amsterdam: Elsevier, Volume 122, 2022, ISSN 0167-4048. p. 11.

53 Proposal for a Directive (EU) on the resilience of critical entities. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829 (accessed on 23 December 2022).

54 See the explanatory memorandum accompanying the RCE Directive, p. 1–2.

55 Annex III to AI Act.