Data protection in a GDPR era: An international comparison of implications for autonomous vehicles

Federico Costantini [a, *], Nikolas Thomopoulos [b], Fabro Steibel [c], Angela Curl [d], Giuseppe Lugano [e], Tatiana Kováčiková [e]

[a] Department of Law, University of Udine, Udine, Italy
[b] Department of Tourism and Transport, University of Surrey & WISE-ACT Chair, Guildford, United Kingdom
[c] Institute for Technology and Society of Rio de Janeiro, Rio de Janeiro, Brazil
[d] University of Otago, Dunedin, New Zealand
[e] Department of International Research Projects, University of Zilina, Žilina, Slovakia
* Corresponding author: *Email address:* federico.costantini@uniud.it (F. Costantini)

Contents

[ac] Input provided by Klar and Vlk (2019).
[ae] Input provided by Steibel and Silva (2019).
[ag] Input provided by Stergiadis et al. (2019).
[ah] Input provided by Costantini (2019).
[aj] Input provided by Curl (2019).
[am] Input provided by Lugano and Kováčiková (2019).
[ao] Input provided by Kyriadikis (2019).

Advances in Transport Policy and Planning, Volume xx
ISSN 2543-0009, https://doi.org/10.1016/bs.atpp.2020.02.005

Abstract

Due to the extensive amount of data generated by an autonomous vehicle (AV) and the information flowing among AVs and through surrounding infrastructure, data governance legislation poses as a significant challenge especially in the perspective of their large-scale introduction. Regulation (EU) 2016/679, which is known as GDPR and entered into force in May 2018, has been a tipping point in personal data protection even in countries outside the European Union (EU). Although the majority of EU member States have already adapted their legal systems to its provisions, a few others are still on the process, and institutions and companies are challenged by the need to comply. This chapter conducts a mapping review of existing regulations in seven countries, namely Austria, Brazil, Greece, Italy, New Zealand, Slovakia and Switzerland, to assess policy challenges of AV testing and deployment focusing on the implications in terms of data protection. Potential areas of cooperation are identified, as well as evidence of divergent approaches, which are discussed in order to provide valuable suggestions for policy making at local, European and international level for AV testing and deployment.

Keywords: GDPR; Data protection; International comparison; AVs trials; Regulatory sandboxes; Living labs

1. AVS AS DISRUPTIVE TECHNOLOGIES: A BRIEF OVERVIEW ABOUT TRANSPORT POLICY CHALLENGES

Information has become more important and valuable than ever, with some stating that data might be considered as the currency of the 21st century (Floridi, 2014; Harari, 2018). Even in transport, data are equally vital as vehicles and infrastructures for the seamless operation of advanced systems and deriving business eco-systems rapidly grown around them (Costantini et al., 2019; Floridi, 2019b; Thomopoulos et al., 2015). It can be argued that as the concept of transport, originally bound to the physical displacement of passengers and freight, is turning into a more sophisticated, inclusive and incorporeal concept, the automotive industry is being transformed from hardware- to software-focused (Kováčiková, 2018).

Concurrently, in the attempt of addressing those emerging technologies (Rotolo et al., 2015), legal frameworks are facing equally profound transformation (Lugano et al., 2019). Indeed, in developed countries In-

formation and Communication Technology (ICT) has been required to protect data sources and communication since the beginning of the 21st century. Such frameworks have been also linked with advancements within the Intelligent Transport Systems (ITS) sector. The contemporary EU (European Union) regulation in ITS is underpinned by the Directive 2010/40/EU,[a] the Delegated Regulations based on it—namely Delegated Regulation No 305/2013,[b] No 885/2013,[c] No 886/2013,[d] No 2015/962,[e] No 2017/79[f] and No 2017/1926[g]—besides the EU Regulation 2015/758[h] and two European Commission decisions.[i]

[a] Directive 2010/40/EU of the European Parliament and of the Council of July 7, 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 (OJ L 207, 6.8.2010, p. 1–13).

[b] Namely, Commission Delegated Regulation (EU) No 305/2013 of November 26, 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonized provision for an interoperable EU-wide eCall (OJ L 91, 3.4.2013, p. 1–4).

[c] Commission Delegated Regulation (EU) No 885/2013 of May 15, 2013 supplementing ITS Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles (OJ L 247, 18.9.2013, p. 1–5).

[d] Commission Delegated Regulation (EU) No 886/2013 of May 15, 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users (OJ L 247, 18.9.2013, p. 6–10).

[e] Commission Delegated Regulation (EU) 2015/962 of December 18, 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21–31).

[f] Commission Delegated Regulation (EU) 2017/79 of September 12, 2016 establishing detailed technical requirements and test procedures for the EC type-approval of motor vehicles with respect to their 112-based eCall in-vehicles systems, of 112-based eCall in-vehicle separate technical units and components and supplementing and amending Regulation (EU) 2015/758 of the European Parliament and of the Council with regard to the exemptions and applicable standards (OJ L 12, 17.1.2017, p. 44–85).

[g] Commission Delegated Regulation (EU) 2017/1926 of May 31, 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services (OJ L 272, 21.10.2017, p. 1–13).

[h] Regulation (EU) 2015/758 of the European Parliament and of the Council of April 29, 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (OJ L 123, 19.5.2015, p. 77–89).

[i] Namely, Decision No 585/2014/EU of the European Parliament and of the Council of May 15, 2014 on the deployment of the interoperable EU-wide eCall service (OJ L 164, 3.6.2014, p. 6–9), and Decision (EU) 2017/2380 of the European Parliament and of the Council of December 12, 2017 amending Directive 2010/40/EU as regards the period for adopting delegated acts (OJ L 340, 20.12.2017, p. 1–3).

In this context, the recent global expansion of AVs[j] represents a potential disruptive innovation (Christensen and Bower, 1996; Christensen et al., 2015; Yu and Hang, 2010).[k] Indeed, as many other technologies currently being introduced and tested worldwide, such as artificial intelligence (AI), cloud computing, distributed ledger technology (DLT), AVs promise a revolutionary impact on the transport and mobility sectors (Hogan and Helfert, 2019; Hogan et al., 2019), presenting extraordinary opportunities, as well as many concerns in different fields (urban development, transport equity, environmental sustainability, labor market, cybersecurity, data protection) as some studies recently pointed out (Alavi et al., 2018; Blyth et al., 2016; Floridi, 2019a; Ronzhyn and Wimmer 2019). As a matter of fact, an increasing number of vehicle manufacturers are already entering this market, along with multiple city authorities aiming at reaping potential benefits (Milakis et al., 2017; Thomopoulos and Givoni, 2015) and a lot of initiatives have been already adopted by the EU or are currently in progress concerning *Cooperative Intelligent Transport Systems* (or also "C-ITS") according to COM/2016/766.[l]

Since effects of disruptive technologies are uncertain, and consequences could be impossible to control potentially irreparable large-scale damages, in recent years governments are tackling disruptive technologies with a new kind of legislation, namely "regulatory sandboxes." Indeed, legal provisions are enacted specifically to create restricted environments where, under given conditions, new technologies along with relevant regulations are tested, minimizing the risk of drawbacks (Zetzsche et al., 2017). Despite that "regulatory sandboxes" could be the most suitable tool for legislators to manage uncertainty, it has to be said that such initiatives *per se* do not exclude the possibility of unexpected outcomes but certainly increase the complexity of legal frameworks, which are already challenged by others factors, such as the multiplication of legal sources brought by globalization and regionalism, as well as the risk of different treatment for the same cases brought by the fragmentation of jurisprudence. Consequently, uncertainty, which is inevitable in a

[j] Although no consensus exists among academics and practitioners regarding the definition of AVs, this chapter focuses on wider data management and protection issues which are intertwined with highly automated or fully automated, i.e., autonomous vehicles. Therefore, no attempt is made to define the term AV more precisely since this is beyond the scope of this chapter, but may as well be addressed within this book.

[k] In this chapter we use the concept of "disruptive technology," which is widely accepted, since others, as "emerging technologies," are debated among scholars (Rotolo et al., 2015).

[l] COM/2016/766 final of November 30, 2016. *A European strategy on Cooperative Intelligent Transport Systems, a milestone toward cooperative, connected and automated mobility*.

complex legal system, could be increased by the introduction of "regulatory sandboxes."

This approach has been adopted by several countries also in Europe. Indeed, apart from "Living Labs" which have been introduced for mobility and IT services for a number of years already,[m] new ones have emerged in Slovenia,[n] Spain[o] and the UK.[p] Such sandboxes include advanced AV proving grounds realized in Sweden[q] and Hungary[r] (Alonso Raposo and Ciuffo, 2019), while a range of other similar grounds are under development. On this account it is important to underline that it is the EU suggesting the implementation of "regulatory sandboxes" in fields where AI could be deployed with unpredictable consequences, as stated in COM(2018) 237 of April 25, 2018, *Artificial Intelligence for Europe* (p. 9). Specifically, the development of testing facilities where AVs can be safely experimented is encouraged in COM(2018) 795 of December 7, 2018, *Coordinated Plan on Artificial Intelligence* (Annex, p. 8) and in the High Level Expert Group Policy *Investment Recommendations for Trustworthy AI* of June 26, 2019 (p. 27), and endorsed in many initiatives at a national level such as the one adopted by Germany (German Federal Government, *Artificial Intelligence Strategy*, November 2018).

Data governance in ITS and in particular of AVs is crucial, since information is the key not only for implementing technologies, but also for evaluating their social impact and even for establishing policies and thus legal regulation. In addition, it has to be considered that technologies are often applied in combination and in the future they will be even more deeply intertwined—for example, the implementation of DLT in ITS (Hogan and Helfert, 2019; Hogan et al., 2019)—making both their impact more disruptive and their assessment more challenging. Finally, it is important to highlight that the data relating to AVs can differentiate not only by nature (personal and not personal data, as elaborated in the next section) but also by content (ordinary working conditions of ITS or test results of AVs). Therefore it is necessary to shape an innovative approach that encompasses all these considerations putting them into practice.

[m] (SUNSET WP7 2013, www.sunset-project.eu).
[n] http://avlivinglab.com.
[o] http://catalonialivinglab.com.
[p] https://www.smartmobility.london.
[q] http://www.astazero.com.
[r] https://zalazone.hu.

2. DATA PROTECTION AND AVS: IMPLEMENTING GDPR IN THE EU AND COOPERATING WITH OTHER COUNTRIES

It is noteworthy that the aforementioned legal provisions are integrated with others about cybersecurity and data protection, such as Directive (EU) 2016/1148 "Network Information Security" (also "NIS"),[s] Regulation (EU) 2016/679 ("General Data Protection Regulation," henceforth GDPR),[t] Directive (EU) 2016/680,[u] Directive (EU) 2016/681[v] and the most recent EU Regulation 2018/1807[w] concerning the free flow or non-personal data, which entered into force on May 29, 2019. Further provisions are anticipated to be enacted when EU Directive 2002/58 will be repealed by a regulation which was under discussion in 2019.[x]

GDPR is the prominent legislation regarding data protection within the EU, setting also a global standard, as it represents the backbone of the future EU digital economy. Indeed, GDPR replaces previous Data Protection Directive 95/46/EC,[y] introducing several crucial improvements (Voigt and Von Dem Bussche, 2017), rewriting former fundamental principles and complementing them with the requirement of account-

[s] Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1–30).

[t] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1–88).

[u] Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

[v] Directive (EU) 2016/681 of the European Parliament and of the Council of April 27, 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime (OJ L 119, 4.5.2016, p. 132–149).

[w] Regulation (EU) 2018/1807 of the European Parliament and of the Council of November 14, 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59–68).

[x] COM (2017) 10: Proposal for a Regulation Of The European Parliament And Of The Council 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), Procedure 2017/0003/COD.

[y] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31–50).

ability (article 5, Section 2), which becomes the cornerstone of GDPR compliance. Furthermore, it imposes new obligations for the Data Controller, such as the "Data Breach" notification (articles 33 and 34) and the Data Impact Assessment (article 35), while introducing new roles as the Data Processor (article 28) and the Data Protection Officer (articles 37–39). Third, it increases the rights of the Data Subject establishing new prerogatives, including the "right to be forgotten" (article 17), which before was only declared by the notorious decision "Google Spain."[z] Lastly, it reorganizes the institutional network of European and national authorities (Chapter IV), while redesigning the criteria for assigning and assessing responsibilities in case of infringement (Chapter VII). In sum, GDPR paves the path for an advanced legal framework in personal data protection, setting an international standard concept of data governance.

Under the GDPR regulation, institutions and companies can ensure risk management and process optimization (Gellert, 2018) adopting a proactive approach toward incoming technologies, particularly about the Internet of Things and Artificial Intelligence (Pagallo et al., 2019; Wachter, 2018; Wiatrowski, 2018). Indeed, efficient data management brings together essential people, processes, and technologies to safeguard increasingly understandable, accurate, complete, reliable, secure, and discoverable data, thus protecting business assets and supporting economic growth.

Within this rapidly changing context, data collection and processing through AVs raises multiple legal issues depending on the information management framework in place, no matter if it takes place within controlled environments (e.g., proving grounds) or within public space (e.g., public roads).

In the first case, it can be observed that the main principle is confidentiality, which is applicable for any type of data. Among them, a peculiar category is represented by "personal data," which are related to identified—or identifiable—physical individuals. Despite that some rights are granted to drivers, passengers or pedestrians as "*data subjects*" (article 4(1) GDPR), in principle the ownership of such data is entitled exclusively to those who ultimately control them, and so are defined as the "*Data Processor*" (article 4(7) GDPR). According to Delegated Regulation (EU) 2015/962, "*accessibility, exchange and re-use*" of special kinds

[z] Judgment of the Court (Grand Chamber), May 13, 2014, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317.

of data, specifically "static road data" (article 4), "dynamic road data" (article 5) and "traffic data" (article 6) have to be granted. Furthermore, an EU regulation defines the technological standard to be adopted for data transmission, which is currently DATEX II.[aa] The key purpose of such provisions is naturally road safety, which constitutes a primary objective nationally (e.g., Sweden, UK) or internationally (e.g., EU).

In the second case, data are crucial for AV deployment both within public space and within Living Labs, since they embody precisely the purpose of such experiments. As it can be easily imagined, also due to the huge investments made to design, build and maintain vehicles, onboard devices and infrastructure, the value of respective findings achieves a strategic importance not only in terms of pure research outcomes, but also of industrial production and even of geopolitical strategic needs. On one hand, the general interest in sharing the final results of public funding may be prioritized or, at least, allowing interested parties to take an indirect advantage out of them. On the other hand, there is a legitimate expectation of a proportionate benefit by those who contribute in the early stages of such endeavors and investments. Data management and protection is unsurprisingly placed at the core of this challenge, since investors would be entitled without exceptions granting any "accessibility, exchange and re-use"—or else—to the general public or to third parties.

All of the legislation previously outlined may be suitable in addressing past or contemporary challenges, yet it is largely unknown whether it will be fit for purpose in addressing with the same efficacy the forthcoming disruptive innovations including AV deployment. Due to the increased significance of data in emerging AV value chains, the regulatory frameworks surrounding AVs and AV trials, particularly about ethical, legal and social (ELS) challenges, are still at an embryonic stage. Aside a handful of US states (e.g., Arizona, California, Nevada) and European countries (e.g., UK) which have already introduced the first wave of relevant regulations, most countries are still adapting to the broad requirements of GDPR or their equivalent national legislation. However, given the vast volume of data that would be generated daily by AVs, it is critical to formulate such regulations. Moreover, it is essential to foster cross-country collaboration regarding data management not only in the EU where many member states are closely interconnected, e.g., through a borderless area (Schengen area), but also internationally across countries

[aa] https://datex2.eu/.

and continents. Due to existing global supply chains of vehicle manufacturing and since vehicle manufacturers already state in their Terms and Conditions of sale that all vehicle generated data is owned by them, it is apparent that this is a field of international concern for both practitioners and policy makers.

Therefore, this chapter reviews existing data protection regulations and policies directly related to ICT, transport and AV regulations as well as policies in different countries and continents, namely Austria, Brazil, Greece, Italy, New Zealand, Slovakia and Switzerland to assess policy challenges of AV deployment and the deriving data management and protection implications. New mobility services are used as a proxy for the policy and regulatory context in an AV and GDPR era. Through this mapping review, it highlights cross-country similarities and variations focusing on key implications for AVs, classified in selected categories. Ultimately, this synthesis chapter (van Wee and Banister, 2016) contributes in identifying contemporary synergies and gaps in advance of any widespread deployment of AVs globally. Through an in-depth review of contemporary practice (e.g., sandboxes) and policy informing indices (e.g., AV Readiness Index—KPMG, 2019), it offers valuable insights, particularly for policy makers in non-car manufacturing developed countries as well as for those in the Global South who are in some ways at the mercy of data protection regulations in the country of vehicle manufacture.

The remainder of this chapter is structured as follows: Section 2 outlines the methodology applied; Section 3 presents the findings of the expert survey conducted in the countries in focus; Section 4 discusses these findings and highlights upcoming challenges; Section 5 concludes, offering policy relevant recommendations.

3. METHOD

Conducting a literature review is a task with its own challenges, particularly in an emerging field of global interest (van Wee and Banister, 2016). However, conducting a literature review about an emerging topic of global interest is even more challenging due to the lack of sufficient quantity and quality of literature to review. Consequently and due to the focus of this chapter on regulatory and legal aspects, the choice has been to focus on a review of relevant local, national and international regulations.

A structured survey questionnaire with closed and open questions was distributed by the authors to selected WISE-ACT[ab] experts who are familiar with both the transport and regulatory challenges of AV deployment, as well as with relevant data management and protection context in their respective countries. These experts are affiliated with European research networks, national research institutes, national transport authorities, NGOs (Non-Governmental Organisations), and Universities. This mix of affiliations both in the Global South and North ensures not only a wealth of expertise, but also diverse stakeholder perspectives depending on the objectives of each expert's affiliated organization. The survey was divided in three sections:

- Data protection regulations;
- AV-related regulations;
- New mobility services regulations.

The choice of countries was based on multiple concurring criteria: review and assess AV data management and protection regulations in a range of countries of variable size across continents, with or without car manufacturing firms in their territory which are represented in WISE-ACT. The selected countries are mentioned in Table 1. Three of them (Brazil, Italy and Slovakia) have car manufacturers in their territory, including some which are foreign-based firms. New Zealand does not have a traditional vehicle industry, but has an AV developer. The selection was made after cautious consideration and the understanding that car manufacturing countries which are at the forefront of AV deployment—such as China, Germany, Japan, Sweden, the UK, the USA —already have been putting structures in place to address relevant challenges. Less attention and progress has been paid to date on the challenges of countries with diverse size, available infrastructure and stage of economic development, hence this chapters aims at covering this gap in both the literature and practice.

Therefore, a mapping review (Grant and Booth, 2009) was identified as the most appropriate method for the review in this chapter. The key objective of mapping reviews is to map out and categorize existing sources, which can then be used as the foundation for further in-depth "*reviews or primary research by identifying gaps in the […] literature*"

[ab] WISE-ACT (Wider Impacts and Scenario Evaluation of Autonomous and Connected Transport) is a COST Action consisting of more than 150 participants from 38 COST Countries, 3 International Partner Countries, as well as the Joint Research Centre (EU) (2019): https://www.cost.eu/actions/CA16222.

TABLE 1 Experts' survey overview of AV deployment data management and protection.

Question no.	Question	Austria	Brazil	Greece	Italy	New Zealand	Slovakia	Switzerland
2	Is GDPR (or similar) implemented in the country?			[a]				
3a	Is there a legal framework in the country about managing mobility data?				[a]			
3b	Do these mobility data legal framework(s) include provisions about AV data?	[a]		[a]				
4	Is there AV specific legislation in the country?			[a]				
5a	Is AV testing allowed in the country?							
5b	Is there any specific provision about AV testing data ownership and management?	[a]						
6	Is there a specifically assigned Authority/ Department at national/regional/local level focusing on AV legislation and policy in the country?							
7a	Is any vehicle manufacturer established in the country?							
7b	Do their vehicle sale T&Cs include a specific clause about data management?							

TABLE 1 (Continued)

Question no.	Question	Austria	Brazil	Greece	Italy	New Zealand	Slovakia	Switzerland
7c	Does this comply with GDPR (or similar) already?							
8a	Do new mobility services providers (e.g., Uber) operate legally in the country?	[a]						
8b	Is there any relevant legislation/case regarding new mobility services (type) data management/protection/sharing?							
8d	Have there been any relevant fines to date?							
9	Is any other new mobility service provider operating in the country?							
9c	Do their service use T&Cs include a specific clause about data management?							
9d	Does the new mobility service comply with GDPR (or similar)?		[a]		[a]			

Gray highlight = positive answer.
[a]Positive answer with special arrangements in place regarding the specific matter.

(Grant and Booth, 2009, p. 94). A feature of this method is that it is constrained according to the determined and available time and resources, while it does not require a formal quality assessment of sources used. Eventually, it aids in identifying areas for further primary or secondary research, which is perfectly aligned with the objectives of this chapter.

4. FINDINGS

This section presents the findings of the experts' survey, highlighting the variation identified among the selected countries regarding AV data management and protection regulations. A summary of those variations is presented in Table 1, followed by an in-depth review of the context in each country.

4.1. Austria[ac]

There are data protection provisions through national legislation, i.e., BGBl. I Nr. 165/1999 and its updated version BGBl. I Nr. 14/2019, which, however, does not specify the level of fines despite allowing claims for damages.

AV testing is permitted in the country (BGBl. II Nr. 402/2016 update BGBl. II Nr. 66/2019 "AutomatisiertesFahrenVerordnung") and mobility data are managed according to BGBl. I Nr. 38/2013 "IVS Gesetz." The national authority responsible for AV deployment is the Department for Mobility Transformation and Transport Decarbonisation within the Federal Ministry for Transport, Innovation and Technology (BMVIT), while AustriaTech is the National Contact Point for Automated Mobility. Relevant regulations specify the traffic situations, road types and speed range within which AV trials and driving assistance systems may be tested. Three test use cases had been possible in 2019 after submitting an application to the BMVIT:

- Automated mini-buses;
- Motorway pilot scheme with lane-change;
- Self-driving military vehicles.

These test use cases are being reviewed. Two applications have been granted permission by 2019: the first concerning valet parking, the second a motorway assistant with automated lane keeping. The existing Code of Practice offers additional assistance to vehicle manufacturers

and AV trial organizers in order to progress from system development to vehicle production. Yet, the only AV data specific provision is about the data generated by the accident recorder which every AV is required to be equipped with. Austria is unique among the set of selected countries since another paragraph is dedicated to the handling of video material which is generated during AV trials.

New mobility services such as Uber are regulated at a provincial level, e.g., in Vienna LGBl. Nr. 36/2011 (GesamteRechtsvorschriftfür Wiener Taxi-, Mietwagen- und Gästewagen-Betriebsordnung) which is based on the BGBl. Nr. 112/1996 (Update BGBl. I Nr. 153/2006) on state level (Gelegenheitsverkehrs-Gesetz).[ad]

4.2. Brazil[ae]

The first Brazilian legislation to reference data protection was issued in 1984, but only after a recent wave of regulations (including the 2011 Access to Information Act, the 2014 Internet Bill of Rights, and the 2018 General Data Protection Law) has the country achieved a strong data protection and privacy rights framework (Aleixo et al., 2019).[af] The current legislation also adopts network security as a principle, and its content relates to security practices, data pseudonymization, and privacy by design. There is no specific legal framework about managing mobility data, although the 2012 Urban Mobility Act establishes, as a priority, the use of collective transportation to cities, including collective and individual mobility, ranging from buses to taxis, and already applied to new mobility services.

Brazil has no AV specific legislation, nor is AV testing specifically allowed or regulated by a specific agency. The 1997 Brazilian Traffic Code Act has no provision for the absence of a driver, which imposes challenges for AV developments in the country. Moreover, Brazil requires the approval and licensing for vehicle circulation from federal and state organizations, as well as for homologation of vehicle components according to technical standards by the National Institute of Metrology, Quality, and Technology (INMETRO) or the Brazilian Association of Technical Standards (ABNT), which introduce additional challenges for AV deployment within the country (Lima et al., 2018).

[ad] The total amount of fines owed by Uber until October 2018 was ca. 680 000 EUR, e.g., https://www.ots.at/presseaussendung/OTS_20180425_OTS0187/entscheidung-des-gerichts-einstweilige-verfuegung-gegen-uber.

[af] https://carnegieendowment.org/programs/technology/cyber/encryption.

The country has a long tradition of car manufacturers, with more than 20 of them established in the county, representing a global range of industries. Uber and other similar mobility smartphone applications have operated in the country since 2014. Such transport modes have no specific legislative provisions, although they are allowed to operate, as ruled by the Federal Supreme Court. Besides Uber, several other ride-hailing, ride-sharing, bicycle and e-scooter services operate in the country. The Terms and Conditions of most smartphone applications provide generic provisions about data management and protection within the country.

4.3. Greece[ag]

The case of Greece is interesting because until 2019 it was one of only two EU countries, to have received a fine by the European Commission for not fully incorporating GDPR in their national legislation. However, some relevant regulations and provisions pre-existed and GDPR has been incorporated in national legislation since September 2019. The Personal Data legislation in Greece was under review until July 2019 pending voting at the national Parliament. So in practice the previous legislation (2472/1976—GGS A 50/10.4.1997) which incorporated the previous EU Directive (95/46/EC) applied as long as it was not against the GDPR. The highest fines imposed in relation to data management and protection (150.000 EUR) have been based on 2472/1997 and 3471/2006 and have been imposed on the four nationally operating telecommunication firms (Decisions 60/2018, 61/2018, 62/2018, 63/2018). A further 150.000 EUR fine has been imposed in 2019 on a large multi-national accounting firm for breaches in employee data management and protection.

Ministerial Decision 50308/7695 has been issued (GN 1837/2015: Terms and Conditions) to operate an urban AV bus (GGS 1837/26.08.2015) which was implemented at the Municipality of Trikala for the experimental application of AV municipal buses within CityMobil2. According to the clauses of that decision, the person in charge or Operator of this AV is perceived as a driver according to the National Driving Legislation in regards to all the administrative, penal and legal responsibilities. It is implicitly assumed that GDPR regulations need to be adhered to and a Data Impact Assessment conducted, but national legislation was not adjusted at that time to allow fine imposing powers to respective local or national authorities.

Although Greece does not have a traditional car manufacturing industry, Tesla opened a small research facility in Greece during 2019. Uber operates certain services in Athens despite some ongoing disputes. Other new mobility service providers as well as a range of ITS (Intelligent Transport Systems) firms exist, including e-scooter operations which were launched in Thessaloniki in December 2018.

4.4. Italy[ah]

In Italy the Legislative Decree "Decreto Legislativo" 196/2003 provides the pivotal legislation in the field of data protection. It is noteworthy that it encompasses not only the incorporation of GDPR, but also of current EU safeguards about privacy in electronic communications, hence data protection in mobile services. Such provisions do not include special provisions regarding AV data.

AV testing is allowed in Italy by article 1 of Law December 27, 2017, n. 205 enforced with a specific bylaw: "Decreto" February 28, 2018 ("Smart Roads" Decree). The first authorization has been issued on May 9, 2019 for AV trials in Turin and Parma. The law does not define the ownership of the data, yet it has provided a detailed list of data which have to be collected (article 12, par. 1 lett. e), and imposes to the car owner to share such data with the public authority for 12 months (article 16, par. 1 lett. b).

The Italian Ministry of Transport has established a special branch specifically devoted to monitor AV testing and developments, called "Osservatorio tecnico di supporto per le Smart Road del Ministero delle Infrastrutture e dei Trasporti." Despite the transformation of FIAT, the historic Italian automotive manufacturing brand, into FCA, no AV manufacturer operates in Italy at the time of writing. FCA has developed a web-based platform which allows customers to create a personal profile. Uber operates in Italy only with some of the services provided worldwide. Namely, UberPop[ai] is not operating after some legal controversies in which the interpretation of the discipline of road circulation was debated (Legislative Decree 285/1992). There are also other mobility service operators, providing different services such as car sharing, car-pooling and bike sharing.

[ai] UberPop was the brand under which in Italy Uber provided the service of connecting private drivers to passengers.

4.5. New Zealand[aj]

New Zealand is unique within this set of selected countries in that it does not have any explicit legal requirement for a driver to be present in a moving vehicle, meaning that there is no legal barrier to testing and fully driverless vehicles (i.e., AV). AVs could be tested on public roads provided they comply with the standard safety requirements. As in other countries, vehicle testing may take place on private land without any third party consent. There are no specific requirements for testing of AV beyond those that would apply to testing any other vehicle. The operator of the vehicle (even if not in the vehicle) must have a driver's license and those undertaking testing must have appropriate public liability and professional indemnity insurance. New Zealand's "no fault" social insurance scheme, funded through the Accident Compensation Commission (ACC) covers personal injury. The New Zealand Transport Agency (NZTA) has outlined a process for applying for testing on public roads—which includes ensuring that vehicles are compliant (or exempted from) with the Land Transport Act, for example, if they have been modified. New Zealand has an additional unique feature since AV trials for air transport (i.e., drones) are permitted in the country.

New Zealand does not have a traditional car manufacturing industry, but there is one AV company. New mobility services are operating in New Zealand including ride-sourcing and micro-mobility. There has been a claim against the privacy act regarding the sharing of information between Uber and the police (Badillo-Lopez vs Uber New Zealand, decided on March 22, 2019).

Legislation regarding data protection provided by the New Zealand "Privacy Act" of 1993 will be repealed and replaced starting from March 1, 2020 by the "Privacy Bill" of 2018. The new legal framework will provide stronger powers, mandatory reporting, new offenses and increased fines. The act is described as having EU adequacy status, facilitating data transfers from the EU to New Zealand, but does not comply entirely with GDPR.[ak] There are mandatory notification requirements for privacy breaches, less requirements on consent, complaints may be raised directly with the company[al] involved, there is no restriction of automated decision making tools, no requirement for privacy by design or

[ak] See the Privacy Bill digest n. 2588 at https://www.parliament.nz/en/pb/bills-and-laws/bills-digests/document/52PLLaw25881/privacy-bill-2018-bills-digest-2588.

[al] The term used in New Zealand's legal framework is "agency."

privacy impact assessment. Data protection in electronic communications is provided by the "Telecommunications Information Privacy Code," which is in force in its revised version since September 28, 2017.

There are no specific provisions regarding data ownership and management for AVs, whereas the Ministry of Transport states that it will monitor and draw on international developments alongside likelihood of commercial availability of AVs.

4.6. Slovakia[am]

In Slovakia, national legislation has been adapted with the entry into force of the GDPR by the Law No. 18/2018 on Personal Data Protection (New DPA). A key actor in data protection is the Office for Personal Data Protection of the Slovak Republic,[an] an independent state authority which performs the supervision of data protection. Citizens can file a complaint to this Office and obtain a statement, which is, however, not sufficient for a decision. Such decisions are taken by the court, to which the complaint may also be filed directly. Hence, statements from the Office for Personal Data Protection are not essential for decisions on these cases. A peculiar aspect of the Slovak system is that people are not used to liability claims as in the UK or the USA. Filing such a complaint is not common and the justice system is generally perceived as slow and with non-transparent procedures.

No specific legislation on AV is available. Generally, the personal data protection legislation is applied as far as it concerns personal data. This gap will be filled in by the Smart Mobility 4-year project, funded through ESIF Structural Funds, managed by the Ministry of Transport and Construction, in collaboration with the office of the Deputy Prime Minister for Investments and Informatisation. This project will develop the legislative and regulatory framework in 2021 and implement it in 2022. Uses of AV data will be covered, including open data and sharing of data.

Four foreign car manufacturers originally from France, Germany, South Korea, UK and one domestic are established in Slovakia. New mobility service providers are also operating, e.g., Uber operates legally in Slovakia since May 2019, after 1 year of suspension of services due to a court decision. This decision established that Uber and any other similar service should fulfill the obligations of any other "regular taxi service" in the country. Even if classified in a different category than taxi service

[an]https://dataprotection.gov.sk.

providers, shared mobility operators are popular. From a legislative point of view, these services fall in a "gray area" since they are presented as "community services" and no court case has been filed yet.

4.7. Switzerland[ao]

The Swiss Federal Data Protection Act (DPA) applies in this country and the Telecommunications Act 784.10 provides the legal framework regarding the management of mobility data. AV trials are permitted on public roads based on Federal Road Traffic Law (SVG) article 106, paragraph 5, however, no special arrangements are in place regarding AV data other than the DPA ones. It is noteworthy that trial authorizations require documentation or confirmation that the legal provisions governing data protection will be complied with, and that data security is assured. The authority in charge of AV trials is the Federal Office of Roads—Federal Office for Spatial Development.

New mobility services operate under local regulations which are issued at a local (Canton) level, e.g., in Lausanne Uber can operate according to the same regulations applicable for taxis and drivers.

5. DISCUSSION AND POLICY IMPLICATIONS

A variety of valuable findings have been identified in the previous section, which are discussed and contrasted hereinafter. It appears that the "GDPR era" has arrived, since all selected countries (Table 1: 2)—and most EU member states—have adopted GDPR or a similar type of legislation recognizing the contemporary significance of data management and protection. Following fines by the European institutions, all EU member States plan to have the GDPR regulation incorporated in their national legislation by 2020. New Zealand on the other hand has a range of unique features, which allow that Country to introduce some type of data management legislation, but not to fully comply with GDPR requirements. Moreover, five out the seven selected countries permit some type of AV trial within their public roads, in addition to AV trials taking place at any private areas which are naturally not restricted. Nonetheless, only two (Austria and Greece) out of the seven selected countries (Table 1: 4) have in place some limited provisions regarding data generated through AV trials.

In contrast, new mobility services are operating in all selected countries. This includes ride-hailing services (e.g., Uber) offered either legally or through indirect channels which has imposed legal battles and fines, as well as other new mobility services such as shared e-scooter schemes. Interestingly, such new mobility services are compliant with GDPR requirements in only two out of the seven selected countries (Table 1: 9d). Therefore, new mobility services appear to be a useful proxy to be used when assessing the data management and protection compatibility of a country or location for AV deployment. The fact that new mobility services are often regulated at a local level (e.g., Austria, Italy, Switzerland, UK), whereas AV trials and data management are regulated at a national level, creates an additional layer of data governance complexity. The latter is particularly important for cross-border collaboration which is common with the EU, e.g., between Austria, Hungary and Slovenia regarding AV trials. A further striking finding is that despite the anticipated importance of AV deployment for freight transport, limited arrangements are already in place about this sector.

At a policy level, it can be argued that aside leading large countries with extensive resources and established automotive manufacturers available, there is no clear policy leadership. In spite of the adoption of GDPR or similar legislation and regulations, awareness and debates among practitioners about AV data management and protection are in their early days. Contemporary familiarization with new mobility services may be useful in raising awareness about both the wider opportunities and challenges among policy makers and the general public.

Overall, this section has highlighted that new mobility services are a contemporary trend, but still the debate surrounding AV data management and protection has not received adequate attention by academics and practitioners to date. GDPR may be perceived either as a "carrot" or as a "stick," but in either case, the focus needs to be diverted in this field too alongside other crucial aspects of AV deployment. Collaboration is essential not only between policies across countries, but also across public and private stakeholders, to shape a liveable future vision including AVs. Consequently, any AV Readiness Index (KPMG, 2019) or other similar index should provide information about data management and protection practice to offer a holistic overview to interested stakeholders.

Table 2 contains a synthesis of the findings, divided by country, concerning actors involved in data protection regulations, AV-related regulations and new mobility service regulations.

6. CONCLUSION AND RECOMMENDATIONS

Based on a mapping review (Grant and Booth, 2009), this chapter has managed to identify common ground and key differences regarding AV data management and protection between the seven selected countries (Table 1). By classifying a range of countries based on their size, economic development stage and whether they host a car manufacturer on their territory, this chapter offers a concise overview of the contemporary legal frameworks and regulations governing mobility data management, AV trials, as well as data generated through new mobility services.

Interestingly, countries outside the EU have already introduced regulations similar to GDPR despite some EU countries are incorporating GDPR in their national legislation in 2019–2020. Data management and protection of AV data is still at a nascent stage, which demonstrates the urgent need to inform users and divert stakeholder focus to this issue. This need is further enhanced by the inherent difficulty in distinguishing between personal and non-personal data. Anonymization is a key factor at this level, but the discussion on such a topic is beyond the scope of this chapter.

Facilitating such a development at an international level is naturally a challenge, but using established *fora* such as UNECE or the EU would certainly enhance relevant efforts. An important finding of this mapping review is undoubtedly that collaboration within and among countries is an indispensable part of the next step of AV deployment. Including the Global South in such developments would naturally constitute a key component of this process, given the rapid urbanization and motorization trends in these countries (Thomopoulos and Nikitas, 2019).

However, only limited resources have been available for this chapter, therefore it is acknowledged that a more comprehensive review is required based on a representative sample of selected countries. If this was to be conducted, then it would mean that the mapping review of this chapter has been useful in identifying a gap for further primary research. Such research could include in-depth interviews with key stakeholders,

TABLE 2 Summary about AV data management and protection in the selected set of countries.

Country	Austria	Brazil	Greece	Italy	New Zealand	Slovakia	Switzerlan
(a) Data protection regulations/*actors* involved	Data protection provisions through national legislation	Data protection and privacy rights framework (2011 Access to Information Act, the 2014 Internet Bill of Rights, and the 2018 General Data Protection Law)	GDPR incorporated in national legislation at the end of 2019	Data protection provisions through national legislation	Data protection provisions through national legislation currently under revision (does not comply with GDPR)	Data protection provisions through national legislation/*Office for Personal Data Protection of the Slovak Republic*	Data protection provisions through national legislation

TABLE 2 (Continued)

Country	Austria	Brazil	Greece	Italy	New Zealand	Slovakia	Switzerland
(b) AV-related regulations/ actors involved	National regulations on AV testing/ Department for Mobility Transformation and Transport Decarbonisation within the Federal Ministry for Transport, Innovation and Technology (BMVIT) and AustriaTech as the National Contact Point for Automated Mobility	No AV specific legislation	No AV national legislation	National regulations on AV testing/ Ministry of Transport	Any explicit legal requirement for a driver to be present in a moving vehicle, no specific provisions regarding data ownership and management for AVs/ Ministry of Transport with a monitoring role	No AV specific legislation	National regulations AV testing/ Federal Offi of Roads—Fed Office for Spatial Developmer

TABLE 2 (Continued)

Country	Austria	Brazil	Greece	Italy	New Zealand	Slovakia	Switzerlan
(c) New mobility service regulations/ actors involved	Regulated at a provincial level	No specific regulation	No specific regulations	National legislation on road circulation (not new mobility services specific)	No specific regulations	No specific regulations	Under loca regulations which are issued at a local (Can level

as well as with individuals directly involved in the legislative process at diverse levels, i.e., local, national, international.

Several issues remain on the background of this scenario. First, the capability to "re-identify" originally anonymous data through AI or Big Data integration with those available publicly is increasing rapidly, challenging current methods of enhancing privacy protection—such as "k-anonymity" (Samarati and Sweeney, 1998) or forced introduction of randomness under a certain threshold of statistical population, or other measures such as "pseudo-anonymization" (article 4(5), 25 and 32 GDPR).

Furthermore, future developments in AI technologies will likely allow AVs to increase their level of autonomy (Russell and Norvig, 2016), yet the legal status of such artificial agents is still under discussion, as confirmed by The European Parliament Report with recommendations to the Commission on Civil Law Rules on Robotics (Delvaux, 2016; Floridi, 2019a). Besides the promising results in the field of "explainable AI," or "XAI" (Adadi and Berrada, 2018), there remains a lack of consensus concerning the property of the data produced by newly developed machines, especially those which can hardly be isolated and separated by the artificial "brains" in which their knowledge is embedded.

Third, the worldwide growth of "regulatory sandboxes" can be seen as an extraordinary opportunity to facilitate the deployment of AVs, yet cooperation among Living Labs is crucial in framing a common approach to AVs and a consistent transport policy. It is noteworthy that in the report "The Future of Road Transport" it is suggested to create a European Network of Living Labs in order to coordinate the efforts for ensuring viable solutions in a field, such as transport, where "*technical and social issues are strongly intertwined*" (Alonso Raposo and Ciuffo, 2019: 43). Establishing multidisciplinary networks of experts such as WISE-ACT is one of the recommended options to make good progress in this respect. The recommendation deriving from the analysis in this chapter is that this approach could help not only to nurture a common vision fostering the development of a harmonized European transport policy, but also to share information such as best practices and outcomes which have a more immediate effect and which can be used to foster public awareness about AVs.

ACKNOWLEDGMENTS

The authors are grateful to the experts in Austria, Brazil, Greece, Italy, New Zealand, Slovakia and Switzerland for their valuable time and input completing our survey. Addi-

tionally, the authors would like to acknowledge the support provided by the WISE-ACT COST Action CA16222 which facilitated the development of this book chapter through meetings, Short Term Scientific Missions and workshops.

REFERENCES

Adadi, A., Berrada, M., 2018. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). vol. 6, IEEE Access, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052.

Aleixo, G., Guimarães Gobbato, A., Garcia de Souza, I., Langenegger, N., Lemos, R., Steibel, F., 2019. The Encryption Debate in Brazil [WWW Document]. Carnegie Endowment for International Peace https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

Alonso Raposo, M., Ciuffo, B. (Eds.), 2019. The Future of Road Transport—Implications of Automated, Connected, Low-Carbon and Shared Mobility. Publications Office of the European Union, Luxembourg.

Christensen, C.M., Bower, J.L., 1996. Disruptive technologies: catching the wave. J. Prod. Innov. Manag. 1, 75–76.

Christensen, C.M., Raynor, M.E., Mcdonald, R., 2015. What is disruptive innovation?. Harv. Bus. Rev. 93, 44–53.

Costantini, F., 2019. Wise-Act Report.

Costantini, F., Archetti, E., Di Ciommo, F., Ferencz, B., 2019. IoT, intelligent transport systems and MaaS (mobility as a service). In: Schweighofer, E., Kummer, F., Saarenpää, A. (Eds.), Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019. Weblaw, Salzburg, pp. 245–254.

Curl, A., 2019. Wise-Act Report.

Delvaux, M., 2016. Report With Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

Floridi, L., 2014. The 4th Revolution. How the Infosphere Is Reshaping Human Reality. Oxford University Press, Oxford.

Floridi, L., 2019. What the near future of artificial intelligence could be. Philos. Technol. 32, 1–15. https://doi.org/10.1007/s13347-019-00345-y.

Floridi, L., 2019. Autonomous vehicles: from whether and when to where and how. Philos. Technol. 32, 569–573.

Gellert, R., 2018. Understanding the notion of risk in the General Data Protection Regulation. Comput. Law Secur. Rev. 34, 279–288.

Grant, M.J., Booth, A., 2009. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info. Libr. J. 26, 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x.

Harari, Y.N., 2018. 21 Lessons for the 21st Century. Jonathan Cape, London.

Hogan, G., Helfert, M., 2019. Transparent Cloud Privacy: Data Provenance Expression in Blockchain. https://doi.org/10.5220/0007733404300436.

Hogan, G., Dolins, S., Senturk, I.F., Fyrogenis, I., Fu, Q., Murati, E., Costantini, F., Thomopoulos, N., 2019. Can a blockchain-based MaaS create business value?. In: Decentralized 2019 Proceedings. https://doi.org/10.3390/proceedings2019028001.

Joint Research Centre (EU), 2019. https://ec.europa.eu/jrc/en/research-facility/living-labs-at-the-jrc/call-expression-interest-future-mobility-and-digital-energy-solutions.

Klar, W., Vlk, T., 2019. Wise-Act Report.

Buzna, , Pourhashem, G., 2018. In: Kováčiková, T., Lugano, G., Cornet, Y., Lugano, N. (Eds.), Intelligent Transport Systems—From Research and Development to the Market Uptake. Springer, Cham.

KPMG, 2019. 2019 Autonomous Vehicles Readiness Index. KPMG.

Kyriadikis, M., 2019. Wise-Act Report.

Lima, D., et al., 2018. https://www.sae.org/publications/technical-papers/content/09-06-01-0004/.

Lugano, G., Kováčiková, T., 2019. Wise-Act Report.

Lugano, G., Hudák, M., Ivančo, M., Loveček, T., 2019. From the mind to the cloud: personal data in the age of the internet of things. In: Zhou, Y., Fischer, M.H. (Eds.), AI Love You: Developments in Human-Robot Intimate Relationships. Springer International Publishing, Cham, pp. 111–130. https://doi.org/10.1007/978-3-030-19734-6_6.

Milakis, D., Arem, B., Wee, B., 2017. Policy and society related implications of automated driving: a review of literature and directions for future research. J. Intell. Transp. Syst. 21, 324–348. https://doi.org/10.1080/15472450.2017.1291351.

Pagallo, U., Casanovas, P., Madelin, R., 2019. The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. Theory Pract. Legis. 7, 1–2.

Rotolo, D., Hicks, D., Martin, B.R., 2015. What is an emerging technology?. Res. Policy 44, 1827–1843.

Russell, S.J., Norvig, P., 2016. Artificial Intelligence: A Modern Approach, third ed. Pearson Education Limited.

Samarati, P., Sweeney, L., 1998. Protecting Privacy When Disclosing Information: k-Anonymity and Its Enforcement Through Generalization and Suppression. Harvard.

Steibel, F., Silva, P., 2019. Wise-Act Report.

Stergiadis, A., Kefalopoulos, M., Thomopoulos, N., 2019. Wise-Act Report.

Thomopoulos, N., Givoni, M., 2015. The autonomous car—a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes. Eur. J. Futures Res. 3, 14. https://doi.org/10.1007/s40309-015-0071-z.

Thomopoulos, N., Nikitas, A., 2019. Smart urban mobility futures, special issue editorial. Int. J. Automot. Technol. Manag. 19 (1/2), 1–9.

Thomopoulos, N., Givoni, M., Rietveld, P., 2015. ICT for Transport: Opportunities and Threats. Edward Elgar, Cheltenham, Gloucester, UK.

Voigt, P., Von Dem Bussche, A., 2017. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer, Cham.

Wachter, S., 2018. The GDPR and the Internet of Things: a three-step transparency model. Law Innov. Technol. 10, 266–294.

Wee, B., Banister, D., 2016. How to write a literature review paper?. Transp. Rev. 36, 278–288. https://doi.org/10.1080/01441647.2015.1065456.

Wiatrowski, A., 2018. Blockchain Technology—A Threat or a Solution for Data Protection? Jusletter IT. 22 February 2018 https://jusletter-it.weblaw.ch/en/issues/2018/IRIS/blockchain-technolog_96aad6c440.html.

Yu, D., Hang, C.C., 2010. A reflective review of disruptive innovation theory. Int. J. Manag. Rev. 12, 435–452.

Zetzsche, D.A., Buckley, R.P., Barberis, J.N., Arner, D.W., 2017. Regulating a revolution: from regulatory sandboxes to smart regulation. Fordham J. Corp. Financ. Law XXIII, 31–103.

FURTHER READING

Glancy, D., 2012. Privacy in autonomous vehicles. Santa Clara L. Rev. 52 (4), 1171–1239.

Lévy-Bencheton, C., Darra, E., 2016. Cyber Security and Resilience of Intelligent Public Transport. Good Practices and Recommendations. ENISA, Heraklion.

New Zealand Parliament, 2018. Privacy Bill Digest. In: https://www.parliament.nz/en/pb/bills-and-laws/bills-digests/document/52PLLaw25881/privacy-bill-2018-bills-digest-2588.

Petit, J., Shladover, S.E., 2014. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 16, 1–11.

Ringe, W.-G., Ruof, C., 2018. A regulatory sandbox for robo advice. In: EBI Working Paper Series.

Schaefer, M.D., 2019. Carpooling and the Pan-European emergency call “eCall 112”: connected cars and their potential for environmental and transport policy. Int. J. Automot. Technol. Manag. 19, 341–369. https://doi.org/10.1504/IJATM.2019.100912.