LEGAL ASPECTS IN DEVELOPING SMART CITY SERVICES AND DATA ECOSYSTEMS

Päivi Korpisaari, Juha Vesala, Shakila Bu-Pasha, Dennis Brouwer, Sara Lehtilä, Oona Ojajärvi, Annika Antikainen

1 Introduction

Legal regulation impacts both enabling factors and barriers with regard to successful implementation of smart city services and related infrastructures. A stable legal framework makes it easier for business companies and municipal operators to plan their actions. It also attracts investment in the sector. Clear, predictable and comprehensible legislation that safeguards people's rights and maintains citizens' trust over the stewardship of their data is also important in order to encourage people to take advantage of the services offered and enabled by smart cities.

The smarter the cities are, the more personal data is collected and used in order to build up and maintain new intelligent services. The Internet of Things (IoT), user location and the use of 5G technology can trigger enormous benefits for network operators and their end users, but at the same time it may create privacy concerns from users' point of view. There is also a risk of hacker attacks against databases and malicious or erroneous data inputs. (Lohan et al., 2018, pp. 281–320)

In these circumstances citizens' trust over lawful processing of data and a sense of security against cyberattacks are of crucial significance. Regulation has to guarantee protection of personal data, a safe and quick network environment, rational and safe use of new technologies, and fair competition. Sustainable development must be supported. On the other hand, legislation should be designed in such a way that, in addition to the objectives mentioned above, it promotes

new innovations and does not unnecessarily hamper the development of services that benefit people and society.

This article considers the legal aspects to be taken into consideration when creating a smart city ecosystem and providing global and local services & data marketplace and related infrastructure.[1] The aim of this text is to describe what regulations and laws apply to the development and discuss whether they help or hinder development. We also look into the future and ponder whether there is a clear understanding of the laws and regulations during the development timeframe, or whether changes in the law are expected. Many fields of law affect the building and functioning of smart city services and not all of them can be discussed in this paper. The focus of this text is on

- personal data protection regulation
- 5G connectivity
- legal and regulatory framework for AI and other emerging technologies
- smart city planning and sustainability
- competition law.

[1] This article is published in a white paper written for the Neutral Host Pilot project, which is funded by Business Finland. Some parts of this article have also been published in the state-of-the-art report written for the same project. More information on the project is available here: https://www.luxturrim5g.com/new-blog/2019/11/4/nokia-driven-luxturrim5g-smart-city-ecosystem-extending (Accessed 21 April 2021). The authors of the article are the following: Päivi Korpisaari, professor (introduction, personal data protection and conclusions), Shakila Bu-Pasha LL. D. (personal data protection), Sara Lehtilä LL. M. and Dennis Brouwer LL.M. (5G connectivity), Oona Ojajärvi LL. B. (legal and regulatory framework for AI and other emerging technologies), Annika Antikainen, law student (smart city planning and sustainability), and Juha Vesala LL. D. and Dennis Brouwer LL. M. (competition law). The authors express their thanks to Heidi Himmanen D.Sc. (Tech) and Annina Lehtonen MSSc, who are officials of the Finnish Transport and Communications Agency (Traficom), for their valuable comments on the 5G connectivity part.

2 Personal data processing in digital services

2.1 Introduction

In order to develop and run global and local services and a data marketplace in a smart city platform, service providers need to collect and process personal data. The Neutral Host platform comprises several participating companies and organisations. We assume two different kinds of processing situations: one that relates to processing data for participating parties' own business purposes, the other relating to selling or sharing data in the Neutral Host data marketplace.

For the first possibility and considering the perspectives of different use-cases of the Neutral Host, the data controllers are business organisations and technology companies that take the initiative to implement smart city use-cases with the authority to determine the purposes and means of personal data processing.[2]

In the second scenario, the Neutral Host will become a controller because it is an individual body that determines the purposes and means of processing personal data. In this scenario the stakeholders deliver personal data for the NHP for its own purposes, namely to enrich, combine and sell data.

It is also possible that a business company together with the Neutral Host will act as joint controllers. According to Article 26 of the GDPR this is the case if "two or more controllers jointly determine the purposes and means of processing." In this case they should transparently determine their responsibilities under the GDPR. Special attention must be paid to the exercise of the data subject's rights and in particular to informing the data subject. The European Court of Justice (CJEU) has interpreted the concept of joint controllership widely. For example in *Jehovan todistajat* the Court concluded that a religious community, such as the Jehovah's Witnesses, was a controller, jointly with its members who were engaged in preaching, for the processing

[2] According to Article 4(7) of the GDPR "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

of personal data carried out by the latter in the context of door-to-door preaching (*Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta*, 2018). In *Wirtschaftsakademie* the Court stated that the administrator of a fan page on Facebook was a joint controller jointly responsible with Facebook for processing the data of visitors to the page, when Facebook was – by means of cookies – collecting and then processing the personal data of visitors. (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, 2018). In *Fashion ID* the CJEU held that joint controllership can exist when a website operator has a role in determining the purposes and means of processing in a situation where it collects data and transmits it to another party who uses it for its own purposes. This website operator could be a controller even if it did not itself have access to the personal data collected and transmitted to the other party. (*Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV,* 2019)

According to Article 26 of the GDPR, joint controllers should transparently determine their respective responsibilities, in particular as regards exercise of the rights of data subjects, as well as their respective duties to provide the information referred to in Articles 13 and 14. Data subjects have the right to exercise their rights under the GDPR in respect of and against each of the controllers.

Considering smart city services and data marketplace, relevant provisions of the GDPR will apply with respect to personal data protection and processing. However, the EU's proposed Data Governance Act[3] is a recent initiative which aims to increase trust in data sharing and promote re-use of public sector data. This would complement the Open Data Directive.[4] Although it is still unclear how this regulation would be effective in accelerating data protection measures, nevertheless the hope is that it will facilitate data sharing throughout the EU and provide advanced solutions for smart city services (Wray, 2020). The Data Governance Act would concern data held by public sector bodies

[3] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

[4] Directive (EU) 2019/1024 of the European Parliament and of the Council on open data and the re-use of public sector information, OJ L 172, 26 June 2019, pp. 56–83.

that is subject to the rights of others. It therefore concerns data that is held by the city of Espoo, but it might help business companies to take advantage of it.

Another solid and trusted legal framework for the protection of personal data, or especially location data is the e-Privacy Directive[5] (amended in 2009)[6] under revision for introduction as the e-Privacy Regulation,[7] effectively complementing the GDPR. This regulation will in particular take into account privacy issues related to electronic communication systems for the Digital Single Market in the EU which will be relevant for smart city services as well. (European Commission, 2020a)

2.2 Risk to personal data, controller's responsibility and DPIA

It is assumed that personal data protection can be affected by use of 5G and other network-based platforms in smart city services because of interconnected networks and smart sensors and devices. According to Article 24(1) of the GDPR, controllers need to "implement appropriate technical and organisational measures" in order to ensure compliance with the regulation. The principle of data protection by design under Article 25 is particularly relevant for a data marketplace such as the Neutral Host where the authorities should take into account appropriate

---

[5] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31 July 2002, pp. 37–47.

[6] Directive 2009/136/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18 December 2009, pp. 11–36.

[7] 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) COM/2017/010 final.

measures at the time of initiating processing operations for protecting data subjects' rights and interests. However, these measures should be decided based on the particular context in question and risks associated with processing, which may include pseudonymisation, preparing a Data Protection Impact Assessment (DPIA), providing information to data subjects with important information regarding processing of their personal data, and so on (European Data Protection Board, 2020a, p. 6).

Article 35(1) of the GDPR requires controllers to carry out data protection impact assessments (DPIAs) if data processing operations – especially applying new technologies – are "likely to result in a high risk to the rights and freedoms of natural persons". The latest technologies used for various services in a smart city platform are supposed to create a "high risk" under Article 35, requiring DPIAs for individual or joint use-cases. Joint controllers can carry out a joint DPIA in suitable situations (de la Torre, 2019). If a set of similar processing operations presents similar high risks, then a single DPIA may be enough in circumstances where it is reasonable and economical. As an example, Recital 92 communicates that: "where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity", a good option could be to initiate a single DPIA.

At the same time, it is pertinent to know who is a processor in different use cases of a smart city. Article 4(8) of the GDPR states, "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". In some situations an entity can be a controller, or a processor, or both at the same time. For example, among different bodies, app developers should be data processors. But in special circumstances they may act as data controllers as well. Controllers and processors should agree on the roles and responsibilities of processors with defined contractual measures. A processor can also contribute to the DPIA considering the nature and availability of information (Article 28(3)(f)). (Bu-Pasha, 2020)

Smart city service providers need to consider some important factors. Controllers have to carry out a DPIA prior to processing. Even if the controllers still do not know all of the processing scenarios, they should plan and sketch these out in the early stage of processing to reflect the principle of data protection by design. This approach is

important and advantageous at the same time because controllers can identify potential risks in advance, which is convenient and cost-effective to manage. Participating companies and organisations of the smart city platform should comply with the requirements of the GDPR and be ready to protect the privacy and personal data of data subjects beforehand. (Bu-Pasha, 2020)

2.3 Consent and contract

Data processing activities can only be lawful if they are covered by the data subject's consent or if there is a legal basis for processing. According to Article 4(11) "consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". According to Recital 42, consent is not considered freely given "if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

Consent must be given meaningfully according to Recital 32 of the GDPR, and the data subject should always have the ability to opt out and withdraw consent any time according to GDPR Article 7(3). Withdrawal of consent should be as easy as giving consent (Article 7(3)). It is up to the controller to prove the existence of consent (Article 7(4)).

Consent is a good legal basis for processing personal data when a person is offered a certain service, for example through a telephone application. This might be, for example, an application that tells you where there are free parking spaces, and to perform this task the service provider can use the location data of the data subject.

When processing special categories of personal data, another justified basis must be stated under GDPR Article 9(2). Consent is one of these bases, so personal data belonging to special categories of personal data can be processed when the data subject has given their explicit consent.

In addition, according to GDPR Article 6(1)(b), data processing will be lawful if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at

the request of the data subject prior to entering into a contract". Such processing should be necessary to execute the contract. Processing is necessary only if the contract cannot be fulfilled without processing the personal data in question. This ground is applicable "irrespective of which phase of the contract is concerned." (Voigt and von dem Bussche, 2017) This ground also allows processing of personal data before the contract is made if the data subject has asked for it.

2.4 Legitimate interest

Regarding some smart city services, asking for consent or entering a contract with every person would be impossible or highly impractical. A "legitimate interest" for processing may be a good ground for processing in many of those cases.

According to Article 6(1)(f) of the GDPR, processing personal data will be lawful if the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." Data controllers carry the burden of proof of their legitimate interests. This ground for processing also justifies processing activities carried out in the interest of a third party. For example, companies may process personal data if it serves the legitimate interests of their customers or clients.

This provision on legitimate interest will not apply to public authorities for processing personal data conducted during performance of their tasks. In addition, careful consideration and documentation regarding processing of data related to children has been emphasised.

To comply with this provision, and in applying the legitimate interest ground, it is recommended that the authorities concerned should test these three elements:

a. Purpose test or identifying the legitimate interest: The interests of the controller or of third parties including corporate interests, individual or wider societal interests can constitute legitimate interests.
b. Necessity test or finding that processing is unavoidable to achieve the purpose: Data processing by adopting legitimate

interests must be necessary, constituting targeted and proportional means of processing. If some other ground appears more reasonable to process the data, legitimate interest will not apply.

c. Balancing test, which means balancing controllers' legitimate interest with data subjects' rights, freedoms and interests: Controllers cannot process personal data if data subjects' rights and interests prevail against the controller's interest. Absence of data subjects' reasonable expectation, or possibility of causing unjustified interference by processing, would weaken the controllers' legitimate interests.

The more compelling and justified the controllers' legitimate interests are, the less probable it is that they will be overridden by the rights and interests of the data subjects. (ICO, 2017) Recital 47 of the GDPR states that data subjects' reasonable expectations based on the relationship with the controller should be taken into consideration. As Voigt and von dem Busshe write, "processing pursuant to Art. 6 Sec. 1 phrase 1 lit. f GDPR shall be lawful if, as a result of a balancing of interests, the legitimate interests of the controller/a third party prevail over the need to protect data subjects" (Voigt and von dem Bussche, 2017). Examples of such relationship are, where the data subject is a client or customer of the controller or provides services to the controller. For example, passengers of robot bus service or users of connected zones are clients of the service providers that act as controllers, and they may reasonably expect that their personal data would be processed and the justification for processing seems compelling.

Furthermore, Recital 47 conveys that processing personal data for direct marketing purposes constitutes a legitimate interest for the controller. Hence, legitimate interest can be a good ground for processing by private entities in appropriate situations.

Different service providing authorities in a smart city ecosystem have to decide which scenarios will match form and apply legitimate interest as a persuasive ground to process personal data. Apparently, and depending on case-to-case circumstances, processing clients' data, processing for direct marketing purposes, transmission of data within participating companies and third parties "for internal administrative purposes" (under Recital 48), as well as fulfilling security purposes (under Recital 49) may appear as possible scenarios to amount to le-

gitimate interest. Moreover, "strategic analysis of customer data to improve the range of products/services or to preserve and attract customers" can serve as a basis for legitimate interest. (Voigt and von dem Bussche, 2017)

Article 6(1)(b) of the GDPR covers only situations where "processing is necessary for performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". This basis may be relied on, for example, when processing the name, address or credit card details of the data subjects to deliver them goods or services. However, the provision must be interpreted strictly, and it does not apply as a legal basis in situations where processing goes *beyond what is necessary* for performance of a contract. Such processing thus needs to rely on another legal basis under Article 6 GDPR. In relation to processing personal data of clients or customers as mentioned above, legitimate interest (Article 6(1)(f)) could provide an appropriate legal basis instead of Article 6(1)(b) when processing of data does not fall within what is necessary for performance of the contract and, for example, when data are processed for direct marketing purposes. (Article 29 Working Party, 2014, pp. 16–18)

Careful assessment is required in applying the legitimate interest ground in relation to data subjects' reasonable expectations, and collection and processing of personal data, so that any misuse of the ground does not take place.

Legitimate interests may intersect with the public interest in some instances. Thus, in addition to having a legitimate business interest, if controllers can show that their operation of the service offers an interest for a wider society which acknowledges the interest, it (the interest) becomes more compelling providing weight to the balancing test and a strong ground to process personal data. (Article 29 Working Party, 2014, p. 35)

As an example, we can discuss the lawfulness of personal data processing by video surveillance. The European Data Protection Board has adopted useful guidelines (European Data Protection Board, 2020b) which cover application of the GDPR in processing personal data through video devices. Video devices may be traditional or smart. Video surveillance has immense implications for personal data protection and privacy, since the question of facial and movement recogni-

tion are involved, which may eventually turn into special categories of personal data.In relation to processing personal data through video devices complying with lawful processing, it is somewhat challenging to implement consent, because huge numbers of people may be monitored through this technology. However, if a controller still intends to depend on consent, it is its responsibility to ensure that the requirements of consent have been properly fulfilled. For the same reason, executing a contract would not be feasible in data processing by video devices. However, legitimate interest and public interest can be lawful grounds for personal data processing in appropriate situations, and the controllers of smart city services can explore the possibility of applying those grounds when suitable and reasonable. (European Data Protection Board, 2020b)

Article 21 of the GDPR contains the conditions for the right to object to processing of personal data when processing is based on the grounds in point (e) or (f) of Article 6(1).

2.5 Public interest

While legitimate interest is a suitable ground for private bodies, public interest can be suitable for public authorities. According to GDPR Article 6(1)(e), personal data processing is permitted if "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

Since the city of Espoo will play an important role in data processing operations in the Neutral Host pilot platform, for example, in implementing the Kera service roadmap, public interest may be a reasonable ground to process personal data. Although this ground is mostly relevant for public authorities, private bodies as controllers can also apply it in appropriate circumstances. In some instances, public and private organisations can jointly implement services which may require personal data processing on the ground of public interest. Services under the Neutral Host can be a good example of such joint endeavours.

The GDPR does not define "public interest". Member States enjoy some flexibilities in defining this concept. According to Recital 45, Member State law can determine the scope of public interest, and which

authorities (public and/or private) can apply this ground. An example of public interest is mentioned in this provision, that is, "health purposes such as public health and social protection and the management of health care services". Processing personal data for the purpose of compiling citizens' political opinions with appropriate safeguards can also constitute public interest (Recital 56).Article 6(3) of the GDPR conveys that the legal basis of public interest should be founded on EU or Member State law. That law should "meet an objective of public interest and be proportionate to the legitimate aim pursued." Article 89(1) states, "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject."

In relying on this ground, it is important to ensure that processing is necessary for carrying out public interest or exercising official authority. For that purpose, the principle of "data minimisation" should be taken into consideration, and processing must be relevant and proportionate to the lawful purpose.

2.6 Does the personal data regulation help or hinder building smart city infrastructure?

Technology develops very fast, and it can be difficult to predict how laws will cope with these developments. In relation to personal data protection, it is a concern for lawyers how the provisions of the GDPR will adjust to current and future technical advancements and realities, and how they impact on creating new data-based services. The GDPR and e-Privacy Directive set certain boundary conditions for legitimate use of personal data and can create some restrictions for use of data. For example, controllers need to fulfil some legal requirements under the GDPR to develop different services in a smart city infrastructure. A flexible interpretation of legitimate interest and public interest as grounds for processing, as well as taking data protection requirements into account even at the design stage of services will ease development of the smart city and its services.

During the lay-out process of this white paper, European Data Protection Board (EDPB) and the European Data Protection Supervisor

(EDPS) adopted a joint opinion on the proposal for a Data Governance Act. (European Data Protection Board and European Data Protection Supervisor, 2021) In their opinion, the EDPB and the EDPS pointed out, inter alia, to the risk that the proposal creates a parallel set of rules, which are not consistent or might lead to possible confusion as to how the proposal would apply together with the existing rules (laid down especially in the GDPR, but also, for example, in the Open Data Directive). Therefore, it would be important to clarify the relation between the proposal and existing legal framework, for example, to guarantee the level of protection of personal data provided under EU law and to ensure legal certainty and consistency of practical application.

It is also important to notice that an adequate level of personal data protection and citizens' trust in legal processing of data and data security raises willingness to share data with the Neutral Host (data marketplace) and take advantage of the many services that service providers in the smart city ecosystem can provide. Informing data subjects about the purposes of data processing and of how and why data is processed, in addition to transparency of the functions of the controller bear an important role in building data subjects' trust.

3 5G Connectivity

3.1 Introduction

The role of connectivity is crucial when building a smart city and operating its multiple 5G services and products. Compliance with telecommunication regulation is a precondition for 5G networks. Telecommunication regulation includes, for example, provisions about licensing procedure and conditions when obtaining or sharing a spectrum licence, obligations and rights which concern companies engaging in telecommunication activities and placement conditions and rights for passive infrastructure. Provisions on cybersecurity need also to be taken into account for the protection of core network functions as traffic in networks includes services vital for the functioning of society. Cybersecurity regulation, for example, imposes obligations on the actors of telecommunication networks to report to the authorities and to notify subscribers and users about any disturbances, information security vio-

lations or threats to information security or other events that prevent or significantly interfere with communication services. Furthermore, EU rules on open internet access must also be complied with by providers of internet access services.

3.2 Applicable laws and regulations

- The European Electronic Communication Code (EECC)[8]
- Finnish Act on Electronic Communication Services (ECSA)[9]
- Finnish Joint Construction Act[10]
- The EU Cybersecurity Act[11]
- Directive on security of Network and Information Systems (NIS Directive)[12]
- EU Open Internet Access Regulation (Regulation 2015/2120, OI Regulation)[13]

The European Electronic Communication Code (EECC) sets the legal framework for telecommunication regulation. The EECC came into force in 2018 and also responds to the needs of 5G networks. Mem-

[8] Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), OJ L 321, 17 December 2018, pp. 36–214.

[9] Laki sähköisen viestinnän palveluista, 917/2014. Unofficial translation of the Information Society Code by the Ministry of Transport and Communications, amendments up to 917/2014 included available at https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf (Accessed 24 February 2021).

[10] Laki verkkoinfrastruktuurin yhteisrakentamisesta ja -käytöstä, 276/2016.

[11] Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7 June 2019, pp. 15–69.

[12] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 July 2016, pp. 1–30.

[13] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance) OJ L 310, 26 November 2015, pp. 1–18.

ber States were obliged to implement the requirements of the EECC in national telecommunication regulation by the end of 2020. The provisions of the EECC promote objectives such as co-investment in high capacity networks, accessibility of networks, and an effective internal telecommunication market (EECC Recital 23). The EECC creates more uniformity in Member States' telecommunication regulation by increasing the level of harmonization concerning, for example, authorization, rights of use and assignment procedure for spectrum licences. Moreover, the EECC has strengthened the influence of EU authorities, namely the European Commission (the EC) and the Body of European Regulators for Electronic Communications (BEREC) (EECC Articles 4, 5 and 10). BEREC has an even more significant role in assisting the work of the EC and in promoting national authorities' convergent implementation of the EECC. BEREC publishes guidelines and reports, and even though this guidance does not have legally binding power, it creates a stronger basis for a common EU approach in the field of the EU telecommunication market (BEREC, 2020b).

The EU Cybersecurity Act aims to secure that critical parts of communications networks are protected carefully in the roll-out of the 5G era. The EU Cybersecurity Act responds to this need by strengthening the competence of the EU Agency for Network and Information security (ENISA) to assess Member States in the field of cybersecurity and by establishing an EU-wide, thus voluntary, cybersecurity certification framework for digital products, services and processes (EU Cybersecurity Act Article 1(1)). The NIS Directive contains provisions on information security obligations and disruption reporting concerning critical infrastructure providers in several sectors, also covering certain digital services. The NIS Directive applies to digital services such as online marketplace providers, online search engine providers, and cloud computing service providers (Traficom, 2019). Moreover, in 2020 the EU created an EU toolbox of risk-mitigating measures for cybersecurity of 5G networks, which is a common survey among Member States for a coordinated EU approach to 5G cybersecurity (NIS Cooperation Group, 2020).

In Finland, the main applicable laws are the Act on Electronic Communication Services and the Joint Construction Act. Finland's telecommunication regulation has a good reputation worldwide. New spectrum bands are implemented quickly and without fiscal goals,

while effective competition among telecom operators also ensures benefits for end-users. The Finnish Transport and Communication Agency (Traficom) is the competent authority in the field of telecommunication networks. The requirements of the EECC have been implemented by reform of the ECSA in 2020. One of the new provisions relevant for 5G operating is the easing of the licensing procedure for local activities. A government-granted network licence is not needed in small-scale public telecommunications services in the case of local activities in a geographically restricted area indicated for such use by government decree. Operating in these areas is covered by a radio licence granted by Traficom (ECSA section 6).

The requirements of the Cybersecurity Act and the EU toolbox of risk-mitigating measures for cybersecurity of 5G networks have also been implemented by reform of the ECSA. For cybersecurity, the reform includes new provisions for the protection of core network functions. According to the new provisions, use of telecommunications devices is not allowed in critical parts of the public network if that can endanger national security. The regulation also applies to micro-operators and providers of private networks connected to certain universal communications networks (ECSA section 244a). Moreover, a new national authoritative body, the advisory board for network security, is founded with a new provision. Its task is to assess and give recommendations on national security in communications networks (ECSA section 244b).

The specific content of telecommunication regulation differs among Member States depending on national implementation of the EECC and the situation in Member States' telecommunications markets. However, the role of EU regulation has strengthened in the field of the telecommunication industry and with the EECC harmonization has increased further. The spectrum for electronic communication services is harmonized at the EU level to enable common markets and use of the same user equipment within and throughout the EU.[14] Harmonization has also been achieved in some frequency bands. The frequency bands identified for 5G in Europe are 700 MHz, 3,5 GHz and 26 GHz.

[14] Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision), OJ L 108, 24 April 2002, pp. 1–6.

Other high bands, 40 GHz and 66–71 GHz, have been identified to be allocated for mobile networks in the future (EECC Recital 135). The EECC also strengthened the level of harmonization in the provisions on radio spectrum licences, for example by lengthening the minimum duration of a licence and prescribing the possibility to extend the validity of network licences granted (EECC Articles 49(1–4) and 50(1–2)). The significant market power (SMP) regulation[15] includes provisions that are more determined by the EU. Member States must, for example, follow EC recommendations and guidelines when defining the SMP position of a telecommunications operator (EECC Recitals 164 and 165).

Telecommunication regulation applies to operators, which means undertakings providing or authorised to provide a public electronic communications network or an associated facility (EECC Article 3(29)). In the context of 5G networks, it is relevant to take into account that, in addition to traditional telecommunications operators, companies providing physical infrastructure for other networks are also subjects of telecommunication regulation. For example, certain rights and obligations concerning joint construction of new infrastructure and joint use of existing networks may also apply to non-telecoms operators if they own or control passive infrastructure useful for operators of electronic telecommunications networks. Moreover, even more actors are subject to cybersecurity regulation. These include, for example, mobile network operators, as well as commercial and non-commercial providers of communications networks and communications services which have not traditionally been perceived as telecommunications operators and associated services and facilities that allow the offer of a communications network or service or supports provision of services.

The OI Regulation applies in the Member States as of 30 April 2016. In Finland, the OI Regulation has been incorporated in the net neutrality provisions of the ECSA. Traficom may provide further regulation to monitor and execute the requirements of the OI Regulation (ECSA section 110). The OI Regulation seeks to introduce common

[15] If telecommunications authorities find that one company can operate almost independently of its competitors, then that company has significant market power in the communications market. In order to secure market balance, such a company can be a target of obligations imposed by telecommunications authorities.

rules to protect equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights, with the aim of safeguarding "the internet ecosystem as an engine of innovation" (OI Regulation Recital 1). The OI Regulation gives end-users an enforceable right to open internet access (OI Regulation Article 3(1)). The term 'end-users' refers to both consumers and business users of internet access services (users) as well as businesses that provide their services through internet access services (Content and Application Providers, or CAPs) (*Telenor Hungary*, 2020, para 37). The right to open internet access entails that users have the right to access the content, applications, and services of their choice, and CAPs have the right to provide these to users via internet access services. Furthermore, the OI Regulation contains the principle of equal and non-discriminatory treatment of traffic for providers of internet access services (Internet Service Providers, ISPs). This means that ISPs are in principle required to treat all traffic within their networks equally and without discrimination in technical terms. ISPs are for example not allowed to block, slow down, or discriminate against traffic of specific services, unless one of the strictly interpreted exceptions in the OI Regulations is applicable (OI Regulation Article 3(3)). BEREC has published guidelines on the implementation of the Open Internet Regulation (BEREC, 2020a), which provide further guidance to national regulatory authorities on how to implement and enforce the provisions in the OI Regulation.

3.3 Does the regulation help or hinder development of 5G connections?

5G sets a new connectivity environment for telecommunication regulation to adjust. Telecommunication regulation needs to balance between the right level of legislative incentives to promote the roll-out of 5G connections and provide sufficient protection for the vital functions of society and for end-users from harmful cyberattacks. Moreover, 5G networks have to be equally available for end-users and customers.

5G networks require dense small-cell base stations and a part of the frequency band to operate a smart city's local activities. There is also more traffic and use for these frequency bands. To run 5G networks, telecommunication regulation needs to enable network sharing agree-

ments, placement and construction rights for passive infrastructure, and effective spectrum policy to an even greater extent. Sharing a network and its elements is estimated to increase as it may also entail cost efficiencies to actors engaging in telecommunication services. Forms of cooperation that telecommunication actors are involved in can be many, and the parties to a sharing agreement might include local companies in addition to traditional telecoms operators. (OECD, 2015, pp. 5–7.)

The EECC and its provisions implemented in the Member States support the new features of 5G connectivity. The EECC sets the framework for national authorities when imposing obligations for telecoms operators for shared use of network elements and co-location of passive infrastructure and the basis for assessing the appropriate level of such obligations. The EECC also imposes requirements on national authorities without undue restrictions to ensure telecoms operators' right for placement and operation of small-area wireless access points, including land or buildings owned by third parties or controlled by authorities (EECC Article 57). Moreover, national authorities have a duty to ensure effective spectrum use and to support licence leasing by appropriate national licensing procedures. With 5G networks, actors engaging in telecommunication network services can be quite varied in addition to traditional telecoms operators. The EECC recognizes these new 5G operating possibilities and thus the scope of telecommunication regulation is extended. (European 5G Observatory, 2020, p. 15)

The level of harmonization and power of the EU authorities in the provisions of the EECC indicates an even stronger impact of EU telecommunication regulation. Uniformity of legislation between the Member States enhances the EU internal communications market and entry of new actors to the communications market may become easier. As deployment of 5G networks is dependent on access to the radio spectrum, harmonization in spectrum bands is crucial. In smart city use cases, when connectivity is required in a local, restricted area but the telecommunications services provided are public, spectrum licensing procedure has also become lighter for this purpose. However, it is still an open question whether the provider of public telecommunication services in a local area is regarded as an operator and what obligations resulting from telecommunication regulation apply.

The EECC aims to promote the EU's competitive roll-out of 5G networks. The legislative trend has been that telecommunications

markets are driven by market forces and remedies of competition law would also apply in the field of the telecommunication industry. Obligations resulting from telecommunication regulation and intervention by the authorities are imposed only if market balance and rights of end-users cannot otherwise be secured (EECC Recital 29). Mainly, sharing agreements of network and infrastructure are based on commercial considerations and the content of agreements is not regulated. However, for example, shared use of passive infrastructure may be mandatory resulting from telecommunication laws (Bourreau, Hoerning and Maxwell, 2020 pp. 14–15). In Finland, the Joint Construction Act, concerning joint use of existing networks and joint construction of new infrastructure, can be applied even if there are no competition concerns.

As 5G networks are expected to become the backbone of many critical IT applications, concerns about more serious cyberattacks are also recognized in cybersecurity regulation. Cybersecurity regulation has been a target of EU and EC legislative motions and proposals. For example, a new proposal for reform of the NIS Directive has been adopted.[16] Provisions on deeper coordination of authorities and more definite provisions on the protected parts of networks as well as notification and reporting obligations are aimed to be updated in the same timeframe as 5G networks take effect (BEREC, 2020b, pp. 8 and 15). Before the inception of the NIS Directive, cybersecurity was not regulated EU-wide. Currently, a common EU approach to cybersecurity has a strong basis (European Commission 2020b).

5G may enable "tailored connectivity" for a number of use cases, including Virtual Reality, Public Safety and Automated Driving (TNO, 2018). Such tailored connectivity may require differential technical treatment of traffic within the networks of ISPs. This has raised concerns among various stakeholders whether 5G connectivity may be at odds with the OI Regulation. BEREC has published an opinion where it considered that the OI Regulation "leaves considerable room for the implementation of 5G technologies" such as network slicing (BEREC, 2018). The reason is that the OI Regulation contains several exceptions

[16] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final.

to the principle of equal and non-discriminatory treatment of traffic. For example, the OI Regulation gives room to ISPs to develop and provide so-called "specialized services" to end-users (OI Regulation Article 3(5)). These are services tailored to the specific Quality of Service (QoS)[17] requirements of specific applications (e.g. Automated Driving) and must meet specific conditions[18] in the OI Regulation.

3.4 Is there a clear understanding of laws/regulation during the development timeframe?

Operating 5G connections is already possible under current telecommunication regulation. Neither EU nor national telecommunication regulation imposes obstacles for the deployment of 5G connectivity. Recent legislative reforms, based mostly on the EECC, can be seen to further support the development of 5G networks. Shared use of networks is allowed and investment in both frequency licences and infrastructure building is supported. A common EU regulatory approach to support the convergent deployment of 5G networks has a strong basis and, for example, the EC's recommendation for best practices to promote investment in networks has recently been issued.[19] The stronger role of the EU authorities and common practices are among tools to ensure the EU's competitiveness against other big countries such as the USA.

In the smart city's connectivity platform, network providers can be separated more at different stages, one providing frequencies, and another base stations. Moreover, new operating models will most likely emerge. Furthermore, sharing agreements and joint ventures among

---

[17] Quality of Service parameters for example include latency, jitter, and packet loss.

[18] See OI Regulation Article 3(5). The most important are that provision of these services must be "objectively necessary" and should not be to "the detriment of the availability and general quality of the internet access service for end-users".

[19] Commission Recommendation (EU) 2020/1307 on a common Union toolbox for reducing the cost of deploying very high capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the COVID-19 crisis in the Union, OJ L 305, 21 September 2020, pp. 33–41.

telecom operators may include new actors in addition to traditional telecom operators, such as local operators, investment companies, and even cities. An open question is how the competent authorities will assess these new forms of cooperation and operating solutions. Case law on 5G connectivity platform implications is still undeveloped. It is relevant to take into account that when estimating the compliance of forms of cooperation and new actors on the connectivity platform, rules of competition law are of high importance (Bourreau, Hoerning and Maxwell, 2020, pp. 46–48 and 83–85). Competition authorities assess whether a joint venture or network sharing agreement among the parties involved is compatible with the telecommunications market. Moreover, in the context of Neutral Host operations, where the idea may be that connectivity is shared on equal terms among the interested parties, principles of competition law such as FRAND-terms[20] are also applicable in the telecommunications field. However, if a sharing agreement or joint venture includes spectrum licence sharing, permissions and conditions for such operation is subject to telecom regulation and approval from the authorities. Moreover, conducting a telecom operator's significant market power decisions and obligations is subject to telecommunication regulation and assessment by the telecom authorities.

Although the EU harmonizes telecommunication regulation even more, there is still certain space for country-specific regulation and assessment by competent national authorities. In particular, frequency allocation and licence permissions are relatively strongly nationally determined. In Finland, the 5G pioneer frequency bands and timeframe for those bands to be deployed are defined by the EECC. However, the allocation and usage of radio frequency bands is defined nationally by government decree (ECSA section 95) and the right to use such bands is subject to national authorities' permission for a spectrum licence. For example, the lower part of the 26 GHz frequency band is reserved for private and local networks in Finland. As the number of frequency bands is limited, obtaining a spectrum licence or cooperation with the licence holder is crucial if aiming to operate 5G services and products. It also influences the conditions for a spectrum licence, what activities can be operated with the licence and the extent of geographic cover-

[20] FRAND-terms; fair, reasonable and non-discriminatory.

age of the licence. Certain geographical areas impose restrictions on the use of frequencies. For example, in Finland, certain parts of the 5G frequency bands are reserved for research, product development and teaching and these bands cannot be used for commercial purposes. Traficom has competence to issue regulations on the use of radio frequencies for different purposes, with due consideration given to international regulations and recommendations on radio frequency use as well as government decree (ECSA section 96).

These national licence conditions and frequency allocation need to be taken into account when developing local services that require 5G connectivity. The strong role of the national spectrum licensing procedure may also affect the entry of international telecom operators and development of local 5G services. However, when securing vital functions of society in the context of radio spectrums is also in question, country-specific regulation can be justified.

In all probability, national regulatory authorities will be confronted with new 5G use cases under the OI Regulation in the years to come. This may result in additional guidance from national regulatory authorities and BEREC as well as case law from the courts, which may further clarify how specific 5G use cases relate to the provisions in the OI Regulation.

To conclude, operating 5G connectivity services in the Kera area is already possible under current telecommunication regulation. Additionally, new implications of 5G connections, such as network sharing agreements, investments in networks and cooperation among different actors are supported within EECC. However, if aiming to engage in telecommunications services in Kera or in some other smart city area, spectrum licence conditions in that area must be paid particular attention. Moreover, if operating 5G services includes joint ventures or network sharing agreements among the parties involved, those activities may need to be approved by the competent authorities, which can vary between Member States. Furthermore, the operative solution and operating local 5G services and products have to be secure from the cybersecurity regulation standpoint. The OI Regulation leaves considerable room for the implementation of 5G technologies. In the future, national regulatory authorities are expected to be faced with new 5G use cases under the OI Regulation, which is likely to result in additional guidance from these authorities, BEREC, and the courts.

4 Legal and regulatory framework for AI and other emerging technologies

4.1 Background

Artificial Intelligence (AI)[21] and other emerging technologies will most likely play a crucial role in the future of smart cities, as they might assist cities and communities to better address the growing societal challenges resulting from, for example, urban concentration and climate change. Due to the high importance and potential of these novel technologies, the question how they should be regulated has also been a topical subject for discussion in the EU and its Member States over the past few years.[22] Various pieces of existing EU and national legislation are in principle applicable and also able to cope with AI and other related technologies. However, due to some specific characteristics of these technologies, the need to assess the applicability of the current framework has been recognised.

The European Commission (the EC) published its first white paper on AI (European Commission, 2020b) in February 2020. The white

[21] There is no precise or universally accepted definition of Artificial Intelligence (AI). Instead, AI is usually defined very broadly. In brief, AI refers to technologies combining data, algorithms, and computing power and the consideration of 'intelligence' (European Commission, 2020b, p. 2). According to one definition provided by the EC, AI "refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (European Commission, 2018, p. 1). Generally, the definition of AI is also divided into (at least) two types: General (or strong) AI refers to systems that can perform most of the activities that humans do, whereas narrow (or weak) AI instead relates to systems that can only perform one of a few specific tasks. For a further developed definition of AI, see, High-Level Expert Group on Artificial Intelligence (2019a).

[22] In 2018 the EC set out an AI strategy (European Commission, 2018a) and agreed on a coordinated plan for AI (European Commission, 2018b) with Member States and Norway to foster cooperation and promote the development of ethical, human-centric and secure AI across the EU. In 2019, the High-Level Expert Group on AI set up by the EC presented non-binding ethical guidelines for trustworthy AI (High-Level Expert Group, 2019b) where it established seven key requirements that AI systems should achieve in order to be deemed trustworthy. In the absence of a common legal framework, some Member States have already taken legislative initiatives to regulate AI.

paper establishes the main principles and prepares the basis for a future common regulatory framework and approach for AI in Europe. Accompanying the white paper, the EC also published a report on the safety and liability implications of AI, the Internet of Things and robotics (European Commission, 2020c) which provides more concrete details on the key implications identified so far for the existing rules on safety and liability. Most recently, in October 2020 the European Parliament (the EP) adopted three resolutions with recommendations on ethical aspects for AI, robotics and related technologies (European Parliament, 2020a), civil liability for AI (European Parliament, 2020b), and intellectual property rights for the development of AI technologies (European Parliament, 2020c). An EC legislative proposal is expected in the first quarter of 2021.

This chapter will briefly outline the evolving EU legal and regulatory framework for AI. It first discusses fundamental rights aspects when developing and deploying AI technologies. Second, the focus is on the product safety and liability framework. Third, the implications of AI for IPRs are assessed.

4.2 EU framework for AI

4.2.1 Fundamental rights

The fundamental rights framework must be carefully reflected and fully complied with when developing and deploying AI-driven technologies. The main instruments of the EU fundamental rights framework are the Charter of Fundamental Rights of the EU[23] (the Charter) and the European Convention on Human Rights,[24] but multiple other legal instruments – international, European, EU and national – also enshrine safeguards for the protection of fundamental rights. A wide range of fundamental rights might be affected around the use of AI, such as hu-

[23] Charter of the Fundamental Rights of the European Union, OJ C 326, 26 October 2012, pp. 391–407.

[24] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended, 4 November 1950, ETS 5.

man dignity, protection of privacy and personal data, as well as equality and non-discrimination. (See, FRA, 2020)

Human dignity (Article 1 of the Charter) is the foundation of all fundamental rights guaranteed by the Charter, and therefore should be adopted as a starting point when developing and deploying products and services relying on AI. The inviolability of human dignity necessitates, for example, that subjecting individuals to AI without their awareness should be avoided. (FRA, 2020, p. 60) Similar values are associated with the fundamental rights of respect for private life (Article 7) and protection of personal data (Article 8) (FRA, 2020, p. 61). Whilst data protection law (notably the GDPR) already contains some rules tackling the risks relating to the use of emerging technologies, additional provisions, for example, related to human oversight and transparency, might be expected in the future to promote trust in these technologies (European Commission, 2020c, p. 9). Concerns for privacy and personal data protection in smart cities can be identified, for example, when deploying facial recognition technologies (see, European Commission, 2020b, p. 21) or when collecting personal data by different kinds of cameras, sensors, and devices placed in smart cities (see, for example, Edwards, 2016). In addition, the fundamental rights of equality before the law (Article 20) and non-discrimination (Article 21) are of significant relevance. Errors or bias in datasets, which are usually difficult to detect and mitigate, may produce discriminatory effects on citizens. (FRA, 2020, pp. 67–68) To address these concerns, the EP in its legislative initiative report published in October 2020, expects, inter alia, that the new legislative proposal should include policy solutions regarding ethical collection of Big Data, algorithmic transparency, and bias (European Parliament, 2020a, paragraph 9).

The EU has highlighted the human-centric approach as a key element of the future regulatory framework for AI. The main objective of the new legislative actions is to find a balance between promoting technological development (and not create disproportionate burdens especially for SMEs) and protecting citizens by addressing risks associated with certain uses of these new technologies. (European Commission, 2020b, p. 17) In order to achieve the objective, the regulatory framework is proposed to follow a risk-based approach, in which the new mandatory requirements would, in principle, apply only to appli-

cations qualified as high-risk. (European Parliament, 2020a, paragraph 12) According to the EP's legislative initiative report, an AI application should be considered high-risk if it meets two cumulative criteria: if both the sector and the specific uses or purposes in question entail significant risks of causing injury or harm to individuals or society (European Parliament, 2020a, paragraph 14). As for applications not considered as high-risk, those would remain entirely subject to existing EU and national provisions.

On the one hand, some of the new mandatory requirements proposed for AI applications qualified as high-risk might hinder the development of such applications, for example, due to higher costs of compliance. On the other hand, ethical and responsible deployment of AI can also be considered as an essential factor to ensure trust in AI-driven products and services. In any case, the risk-based approach aims to ensure that regulatory intervention is *proportionate*. Not all AI applications have an impact on an individual's fundamental rights, and the development of these kinds of applications might not need to follow the fundamental rights-based approach with the same diligence. To ensure more legal certainty, in its legislative initiative report the EP recommends that the EC should develop requirements and indicators for such high-risk technologies, and to issue further guidance on this matter. (European Parliament, 2020a, paragraphs 9 and 50)

4.2.2 Safety and liability

When developing and deploying new technologies, the rules on safety and liability must also be adhered to. These two complementary instruments pursue the same goals of ensuring high safety standards for all products and services, and efficiently remedying damage occurring. The existing EU safety and liability framework, complemented by sectorial rules and national non-harmonised liability legislation, are considered relevant and potentially applicable to a number of novel AI applications. However, the potential implications of AI and other emerging technologies for the existing legislative framework are currently under examination in the EU (see, European Commission, 2020c, European Parliament, 2020b and Expert Group on Liability and New Technologies – New Technologies Formation, 2019).

EU product safety legislation builds on the General Product Safety Directive,[25] and includes a number of sector-specific rules covering different categories of products. The existing framework is already technology-neutral and, in principle, encompasses wide protection against all kinds of risks arising from products. However, it might not explicitly address all the new safety risks that could occur when AI technologies are embedded in products and services, for example risks that result from loss of connectivity, data dependency or opacity ('black box effect') (see, European Commission, 2020c). As another example, it is somewhat unclear whether stand-alone software is covered by the EU product safety rules, as the existing general framework only applies to products, not services (European Commission, 2020b, p. 14).[26] The current legal uncertainty might have its effects on, for example, how products and services including AI can be marketed by operators of the Neutral Host ecosystem. (See, for example, European Commission, 2020b, p. 12)

The Product Liability Directive[27] sets out the general liability regime for defective products in the EU, and allocates liability to the *producer* of a product placed on the market. Sector-specific and national legislation complements the Product Liability Directive, and may, for example, set liability for other players in the supply chain, such as owners, operators, and service providers. (European Commission, 2020c, p. 12) Damage caused by AI or operation of other emerging digital technologies can be compensated under existing laws on damages in contract and in tort in each Member State. Domestic tort laws usual-

[25] Directive 2001/95/EC of the European Parliament and of the Council on general product safety, OJ L 11, 15 January 2002, pp. 4–17.

[26] However, see European Parliament (2020b) paragraph 8: "[The EP] urges the Commission to assess whether the PLD [Product Liability Directive] should be transformed into a regulation, to clarify the definition of 'products' by determining whether digital content and digital services fall under its scope and to consider adapting concepts such as 'damage', 'defect' and 'producer'; is of the opinion that, for the purpose of legal certainty throughout the Union, following the review of the PLD, the concept of 'producer' should incorporate manufacturers, developers, programmers, service providers as well as backend operators [–]". See also Zech (2021).

[27] Directive 85/374/EEC of the Council on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7 August 1985, pp. 29–33.

ly include rules on fault-based liability with a relatively broad scope of application, and several more specific rules regarding for example burden of proof, strict liability, and vicarious liability. (Expert Group on Liability and New Technologies – New Technologies Formation, 2019, p. 16) Even though the existing EU liability framework has functioned well, some specific features of emerging digital technologies are estimated to reduce its effectiveness. Possible challenges relate, for example, to the complexity of products, services and value chains that may result in difficulties in tracing damage back to human behaviour or allocating responsibilities between different economic operators (for instance, liability of suppliers of faulty data). (European Commission, 2020c, pp. 13 and 17 and Zech, 2021)

As a response to the challenges posed by AI to the existing liability framework, in October 2020 the EP adopted a legislative initiative report recommending, inter alia, adoption of a new civil liability regime for AI (European Parliament, 2020b). The report proposes that the *operators* of a high-risk AI-system should be subject to strict liability and to a mandatory insurance regime (see proposed Article 4), whereas products and services relying on AI systems not considered as high-risk should remain subject to fault-based liability (European Parliament, 2020b, paragraph 17), which forms the default principle in all Member States (Zech, 2021).[28] The proposed framework would also apply to AI systems that repeatedly cause incidents resulting in serious harm and damage, even if not classified as high-risk (European Parliament, 2020b, paragraph 21). However, new strict liability rules do not have to be seen as a hindrance for the development of new technologies, but rather as instruments of risk control, at the same time promoting innovation by providing more incentives to further develop technologies to be even safer. Strict liability may thus also increase acceptance of novel technologies. (Zech, 2021) Still, from the viewpoint of operators in the Neutral Host ecosystem, agreements regarding development of AI systems might need to be updated to reflect future developments and potential upcoming liability risks. However, before any law governing the issue of liability is actually passed, some

[28] Simply put, strict liability means that a person (or persons) can be held liable regardless of the absence of fault, whereas fault-based liability arises if the due level of care has not been observed.

lack of clarity will probably remain about expected liability risks. In the context of Neutral Host and Kera smart city services, the applicable national laws are the Tort Liability Act,[29] Contracts Act,[30] Sale of Goods Act,[31]and the Product Liability Act.[32] The application of these relatively old laws in a new technological environment may also lead to some interpretative uncertainties.

4.2.3 Intellectual property rights

Intellectual Property Rights (IPR) rules play an important role in encouraging innovation, as their aim is to give the creators exclusive rights to their intellectual creations. As such, AI poses both opportunities and challenges to the existing IPR framework, whose rules might be of great relevance especially when developing AI technologies and other data-driven solutions.

The existing IPR framework aims at protecting creations of the human mind. That is one reason why the issue whether those frameworks need to be modified due to the emergence of novel technologies is currently being widely discussed. AI systems are usually software-based and therefore typically obtain similar IPR protection to other types of software. For example, patent, copyright and trade secrets protection may possibly be considered, depending on the AI technology in question and on the organisation's IP strategy. However, some typical concerns relate to, inter alia, whether machine-created works or inventions themselves, or AI algorithms can attract protection. To ensure greater legal certainty, the EP in its October 2020 legislative initiative report

[29] Vahingonkorvauslaki, 412/1974. Unofficial translation by the Ministry Justice, amendments up to 61/1999 included available at https://finlex.fi/en/laki/_kaannokset/1974/en19740412_19990061.pdf (Accessed 24 February 2021).

[30] Laki varallisuusoikeudellisista oikeustoimista, 228/1929. Unofficial translation by the Ministry of Justice, amendments up to 449/1999 included available at https://finlex.fi/en/laki/kaannokset/1929/en19290228_19990449.pdf (Accessed 24 February 2021).

[31] Kauppalaki, 355/1987. Unofficial translation by the Ministry of Justice, amendments up to 17/1994 included available at https://www.finlex.fi/en/laki/kaannokset/1987/en19870355 (Accessed 24 February 2021).

[32] Tuotevastuulaki, 694/1990. Unofficial translation by the Ministry of Justice, amendments up to 880/1998 included available at https://finlex.fi/en/laki/kaannokset/1990/en19900694_19980880.pdf (Accessed 24 February 2021).

recommended that the EC should assess the implications of AI and related technologies for current EU legislation on patents, trademarks, design protection, copyright, and related rights (such as the database right), and trade secrets (European Parliament, 2020c, paragraph 10). In addition, the EP also suggested that the EC should support standardisation in the development and dissemination of novel technologies (European Parliament, 2020c, paragraph 11). However, even if the EU is traditionally considered to have a strong IP framework, new measures are sought, inter alia, to help SMEs better manage their IP and to support their competitiveness (European Parliament, 2020c, paragraph 9).

Because data is a vital resource in the data economy, the regulation of data has been the subject of a topical debate in the EU (in this chapter, the focus is on *non-personal* or *industrial data*, rather than on *personal data*, even though drawing the line between these two categories might be difficult in practice due to the wide interpretation of the concept of personal data). As for a basic rule, the EU framework does not grant property rights over data itself, meaning there is no legislation on ownership of data.[33] However, several pieces of legislation somehow affect control of data or data access. These include, inter alia, copyright, database rights, trade secrets and general contract law ('data ownership clauses'). (See, for example, Pihlajarinne and Ballardini, 2019 and Gervais, 2019) While these provisions are critical to protecting ideas and innovations, at the same time they can also create hindrances for data sharing, and thus, also burdens for the development of data-driven products and services. Consequently, the need to strengthen the free flow of data has been recognised in the EU.[34] The EC has also stated in the 2020 European data strategy (European Commission, 2020d) that it will evaluate the IPR framework with a view to further enhancing data access and use (including. for example, the

[33] A data producer's right in 'non-personal or anonymised machine-generated data' (meaning other than personal data) was considered, among other alternatives in the EC staff working document (European Commission, 2017). However, such a right has not been adopted.

[34] See, Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28 November 2018, pp. 59–68.

Database Directive[35] and the Trade Secrets Protection Directive[36]). In addition, the recent EP legislative initiative report stresses the importance of facilitating access to data and data sharing, open standards and open source technology, while encouraging investment and boosting innovation (European Parliament, 2020c, paragraph 15). Moreover, the proposal for a Regulation on European Data Governance (Data Governance Act),[37] which is one of the first adopted measures announced in the European data strategy, aims, inter alia, at facilitating data sharing across different sectors and fostering the availability of public sector data, use of which might be dependent on the rights of others,[38] to enable, for example, pattern detection and machine-learning. (proposal for the Data Governance Act, pp. 1–3) The question how these contradictory objects – limiting or enhancing access to data – will be balanced in the future, remains unanswered at this point.

4.3 Final remarks

To conclude, a number of issues related to AI and other emerging digital technologies are already somehow reflected in the existing legislative and regulatory framework. These requirements must be complied with when designing, deploying, and using AI applications. However, due to recent technical developments, possible gaps in the framework are currently being assessed. The European approach to AI aims at balancing between individual protection and promotion of innovation, but the final consequences of the new legislative initiatives remain to be

---

[35] Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases, OJ L77, 27 March 1996, pp. 20–28.

[36] Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15 June 2016, pp. 1–18.

[37] 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) COM/2017/010 final.

[38] Meaning, for example, data subject to intellectual property or data protection legislation.

seen. To ensure trust in AI-driven products and services, operators in the Neutral Host ecosystem developing, deploying or using AI-based solutions must closely follow the ongoing discussions and be prepared to comply with upcoming adjustments to existing legislation and any AI-specific legal instruments. In any case, these new legislative measures will influence companies relying on AI technologies – especially those considered as high-risk.

5 Smart city planning and sustainability

5.1 Sustainability

5.1.1 What norms apply?

The concept of sustainable development is defined as a development that "meets the needs of the present without compromising the ability of future generations to meet their own needs" (Nations World Commission on Environment and Development, 1987). Norms regarding sustainable development, as with many norms of corporate responsibility, are legally non-binding recommendations and guidelines. These norms are therefore soft-law style standards, the breach of which entails a risk of legitimacy rather than a risk of (il)legality (Ristaniemi, 2020).

Some of these standards are:

- UN Sustainability development goals ('UN SDGs') (UN, 2015)
- Ministry of Economic Affairs and Employment in Finland: Key Guidelines on Corporate Social Responsibility (Ministry of Economic Affairs and Employment in Finland, n.d.)
- OECD: OECD Guidelines for Multinational Enterprises (OECD, 2011)
- UN Global Compact: Guide for General Counsel on Corporate Sustainability Version 2.0. (UN Global Compact, 2019)

The data marketplace will work towards reaching UN Sustainability development goals ('UN SDGs'). It must be borne in mind, though, that while a smart city will have a positive impact on the environment, for example through developing public transportation more conveniently as well as evolving a circular economy, sustainability concerns

not only environment-related topics but also includes economic and social dimensions. (Ristaniemi, 2020) The Neutral Host steers ecosystems towards development compatible with the UN SDGs.

1. *Environmental Sustainability*
   The Neutral Host supports use-cases that are energy-efficient and utilize green energy and pay attention to their carbon footprint. By tracking location data, it is possible to discover roughly how citizens move in the city. This information could be utilized in order to develop more environmentally friendly solutions in traffic.

   An area that supports circular economy innovations presumably attracts residents that share the value of circular economy services, such as a shop selling recycled goods. (City of Espoo, 2020a)
2. *Social Sustainability*
   The Neutral Host offers a platform and a work environment that is open and transparent. It promotes social sustainability by empowering entrepreneurs and by creating more jobs. As a result, it empowers society and facilitates the lives of citizens. The Internet of Things (IoT), for example, enables use of data collected by sensors across the city. Different sensors can also communicate with each other. This data from ecosystems is used in order to accelerate the life comfort of residents in the urban area – some data collected about residents might, for example, be provided through applications to residents. Since a great deal of data is collected, compliance with privacy and security rules, as presented earlier, can also be seen as part of promoting trust and social sustainability, and thus also corporate responsibility.The data marketplace thus steers innovative capacity by creating and allowing new technologies – and the data they have created – to be used and further developed.
3. *Economic Sustainability*
   . The data platform connects small and medium size enterprises (‘SMEs’) based in Finland to the global marketplace. In doing so, the data marketplace thus promotes economic sustainability. The data marketplace, as well as the smart city promotes technological development, invests in new technol-

ogies and utilizes big data in order to develop and increase the efficiency of different parts of urban life.

5.1.2 Future outlook

The Limited Liability Companies Act[39] is being reviewed in case of a need for change, and in its request for an opinion the Ministry of Justice has addressed the issue that, among other things, a need for action on climate change and other sustainability threats have affected companies' operating environment. (Ministry of Justice, 2020) In theory, it might be that sustainable development could be regulated in the Limited Liability Act as well, although a study by KPMG shows that Finnish companies are at the global forefront in how often they include responsibility information in their annual reports. (KPMG, 2020)

There is also an ongoing Sustainable Urban Development Program, and a working group led by the Ministry of the Environment will prepare a proposal for a national sustainable urban development program (Finnish Government, n.d.). There might also be more EU-level legislation regarding corporate responsibility and sustainable corporate governance: the European Commission's Sustainable Corporate Governance Initiative is open for public consultation until February 2021 (European Commission, 2020e).

5.2 Regional and urban planning

5.2.1 What norms apply?

Finnish Land Use and Building Act[40]

The system of land use planning in Finland is regulated so that the Ministry of the Environment has national land use objectives, and re-

[39] Osakeyhtiölaki, 624/2006. Unofficial translation by the Ministry of Justice, amendments up to 98/2011 included available at https://finlex.fi/fi/laki/kaannokset/2006/en20060624_20110981.pdf (Accessed 27 January 2021).

[40] Maankäyttö- ja rakennuslaki, 132/1999. Unofficial translation by the Ministry of the Environment, amendments up to 222/2003 included available at https://www.finlex.fi/en/laki/kaannokset/1999/en19990132.pdf (Accessed 27 January 2021).

gional plans are drawn up by regional councils. Municipalities enjoy a general monopoly regarding both local master plans and local detailed plans. As stated in section 4 of the Land Use and Building Act, the local master plan indicates the general principles of land use in the municipality whereas the local detailed plan indicates how land areas within a municipality are used and built. The local detailed plan is therefore a more detailed land use plan based on the master plan.

Urban planning determines how land is used and may resolve the competing interests of economic development, environmental protection, equity, and social justice (Campbell, 1996). A smart city aims to connect people, information and city elements through technological innovations. Kera area in the city of Espoo has been planned to become an international example area of the circular economy, and existing rail traffic and 5G technology enable implementation of IoT and mobility solutions. (City of Espoo, 2019. See also, City of Espoo, n.d.) Kera is also part of the KIEPPI project which aims at three districts – Kera, Hiedanranta in the city of Tampere and Turun Tiedepuisto in the city of Turku – to develop solutions for circular and sharing economies in an urban environment (City of Espoo, 2020b). Kera will also create urban food production as part of the living urban environment (City of Espoo, 2020a).

Smart city areas have thus already been taken into account in local detailed plans as areas that promote sustainability and innovation.[41] And through the IoT and mobility solutions, the smart city and the data market place aim to facilitate and enhance citizens' quality of life.

5.2.2 Future outlook

A legislative project regarding reform of the Land Use and Building Act (Ministry of the Environment, n.d.) involves planned reform relating to the following objectives:

- building a carbon-neutral society,
- improving the quality of construction,
- promoting digitalization, and
- safeguarding biodiversity.

[41] E.g. Hiedanranta in the city of Tampere has been planned in the planning programme to be a sustainable intelligent and innovative district (City of Tampere, 2020, pp. 13, 28 and 38–39).

6 Competition law

6.1 Competition rules in the EU

EU competition law applies to the economic activities of undertakings such as the Neutral Host Company. The two main EU competition law prohibitions are:

- Agreements and cooperation restricting competition (Article 101 Treaty of the Functioning of the European Union[42], later TFEU).
- Abuse of a dominant position (Article 102 TFEU).

Under both prohibitions, practices may be justifiable by their pro-competitive effects.

The national laws of Member States typically contain similar prohibitions as those under EU competition law.[43] However, Member states are allowed to adopt stricter rules regarding unilateral practices and may thus set stricter rules as regards unilateral conduct than EU law. These prohibitions are enforced by the European Commission and the respective national competition authorities and can also be applied by national courts and arbitrators.[44] In some cases, the Member States also have legislation within or outside competition law that governs the economic activities of undertakings that the competition authorities, courts or other bodies may enforce. In particular, new rules for platforms are being considered in various EU Member States. These would complement existing competition rules, and have already been adopted for instance in Germany.[45]

---

[42] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26 October 2012, pp. 47–390.

[43] See Finnish Competition Act (948/2011), unofficial translation by the Finnish Competition and Consumer Authority / Ministry of Employment and the Economy, available at https://www.kkv.fi/en/facts-and-advice/competition-affairs/legislation-and-guidelines/competition-act/ (Accessed 27 January 2021).

[44] Council Regulation (EC) No 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4 January 2003, pp. 1–25.

[45] 10th amendment to the German Act against Restraints of Competition. Available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s0002.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bg-

Both EU law and the national laws of Member States also have rules on merger control.[46] These rules apply to certain more permanent arrangements (such as joint ventures) or transfers of control over businesses. In practice, these rules mean that undertakings may be required to notify the European Commission or one or more national competition authorities in advance of implementing their joint ventures and transfers of control over businesses. Following notification, the competition authority will evaluate the effects of these transactions on competition and decide whether to prohibit or allow the transaction, or allow it with certain conditions.

Finally, entirely new rules are being considered at the EU level in the fields of competition and other legislation. In particular, the European Commission has recently published a proposal for a new Digital Services Act (DSA) and Digital Markets Act (DMA), which set out a range of new obligations for platforms.[47] Furthermore, the Commission is currently developing a new competition tool (European Commission, 2020f). This seeks to make competition law interventions more effective in the digital economy. In some instances, the new legislation may apply to unilateral conduct by non-dominant undertakings. It remains unclear whether and to what extent these laws will also be applicable to activities of the Neutral Host Company.

6.2 Data platform and marketplace

EU competition law provides limited guidance for the practices of data platforms and marketplaces. There are no clearly defined legal rules and only a limited number of cases have dealt with data and platform-related practices of undertakings. As a preliminary observation,

---

bl121s0002.pdf%27%5D__1611570411206 (Accessed 27 January 2021).

[46] Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings (the EC Merger Regulation), OJ L 24, 29 January 2004, pp. 1–22.

[47] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final; Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final.

EU competition law does not seem to directly help the development of a data platform and marketplace by the Neutral Host Company. However, EU competition law also does not seem to impose fundamental obstacles for the development of data platforms or marketplaces by prohibiting any essential aspect thereof. Moreover, the competition rules may help the Neutral Host Company and its customers by safeguarding against restrictions of competition imposed by others (such as restraints on access to data).

In any event, competition law needs to be taken into account in relation to some specific aspects of the data platform and marketplace. For example, the various agreements involved as well as unilateral practices of the Neutral Host Company (if dominant in any relevant market) are capable of triggering prohibitions in EU and national competition law, and thus need to be carefully designed to avoid the risk that such infringement poses (such as fines and costly investigations, prohibitions against practices). Since as yet there are no established approaches in competition law for some data and platform practices, as noted above, uncertainty remains over how authorities and courts will treat those practices. For example, competition law may create possible risks and uncertainties for some data and platform-related practices of the Neutral Host Company. For instance, it is uncertain what contractual restraints concerning the Neutral Host Company relating to the use of data or access to the platform are acceptable under EU competition law. Another example is that it is unclear under what conditions EU competition law imposes an obligation on the Neutral Host Company to provide others access to its data.

As regards new competition and related legislation under consideration, the proposal by the European Commission for the DMA and the new competition tool may lead to new rules for data-related practices of platforms. For example, the proposed DMA obliges digital gatekeepers to refrain from using any not publicly available data provided by its business users in competition with those business users. However, it is not yet clear whether the data platform and marketplace of the Neutral Host Company will fall within the scope of the DMA. Additionally, the new competition tool may introduce data sharing remedies for identified competition concerns, and new national rules could establish rules relating to data-related practices.

6.3 Connectivity

To provide a 5G connectivity platform, the Neutral Host Company or its customers may engage in infrastructure sharing arrangements with other players, such as MNOs or the City of Espoo. These sharing arrangements can, for example, take the form of a network sharing agreement or a joint venture.

Competition law currently provides little guidance for network sharing agreements between actors other than MNOs. Until now, court cases and decisions and guidance from the competition authorities mostly deal with network sharing agreements between MNOs. In some cases, network sharing agreements between MNOs have been prohibited or have been subject to remedies due to competition concerns from authorities and courts (Finnish Competition and Consumer Authority, 2015). However, the local operator concept differs significantly from directly cooperating MNOs, as MNOs would not directly coordinate their conduct among themselves or share information among each other. Vertical agreements between a local operator and MNOs thus raise fewer concerns than horizontal cooperation between (potentially) competing MNOs. Nevertheless, vertical agreements may raise concerns (for example, restrictions in them) and could nonetheless result in explicit or tacit coordination of MNO conduct. Moreover, the founding and operation of a local operator company may entail cooperation between various undertakings, which may also raise concerns particularly if MNOs are involved that could compete with any of customer MNOs or the local operator itself. Competition concerns can, however, be justified by the undertakings involved by establishing that practices create efficiency benefits that ultimately outweigh the negative effects on consumers. (BEREC, 2019)

When infrastructure sharing or the activities of a local operator takes the form of a joint venture or a transfer of control over businesses, the transaction may need to be notified in advance to the European Commission or one or several national competition authorities. There have been cases where MNOs engaging in such transactions needed to submit commitments to competition authorities to address competition concerns that their joint ventures or other transactions raised (*Vodafone Italia / TIM / Inwit JV*, 2020). In some Member States (for example, Austria), there is also a notification obligation for active sharing agree-

ments between MNOs (Austrian Regulatory Authority for Broadcasting and Telecommunications, 2018).

Consequently, competition law may to some extent hinder the local operator concept due to the risk that cooperation and agreements relating to sharing network assets could trigger investigations by competition authorities or claims in courts. In particular, lack of guidance for network sharing arrangements between parties other than MNOs creates legal uncertainty for local operators as it is not possible to predict at this point how competition authorities and courts will treat practices by which a local operator shares the network or other assets with MNOs. To our knowledge, there are no legislative proposals or guidelines in the EU that seek to address these uncertainties. In some Member States, though, authorities are developing additional guidance for network sharing arrangements between MNOs (for instance, the Netherlands; see, Netherlands Authority for Consumers and Markets, 2019). Some issues related to network sharing arrangements between parties other than MNOs may also be cleared up by competition authorities through future investigations and assessments of notified transactions.

On the other hand, competition law could help the Neutral Host Company to the extent that the local operator concept is regarded as less restrictive of competition than direct cooperation between MNOs. For example, this would encourage MNOs considering sharing of network assets to choose a local operator model in order to minimize the risk of competition law infringement or in order to justify a restriction of competition with efficiency benefits. However, as noted above, it remains uncertain so far how authorities and courts will regard the local operator concept and in which situations it is an alternative to direct MNO cooperation.

6.4 Conclusions and outlook

Both EU and national competition law apply to the Neutral Host Company and all undertakings involved. Competition law does not seem to pose a fundamental obstacle for the development of a data platform/marketplace and connectivity platform. The higher competition law risks associated with network sharing agreements between MNOs may

even favour the Neutral Host Company where the risks of network sharing through a local operator are comparatively smaller. However, competition law does lead to a number of risks and uncertainties for the Neutral Host Company. This is especially because competition law currently provides limited guidance for the Neutral Host company when it wants to engage in data, platform related practices or in arrangements by the NHC or its customers relating to network sharing. Some of the legal uncertainties may be clarified in future case law and decisions and guidance from competition authorities. It remains to be seen to what extent new legislation for platforms in the EU (e.g. the Digital Markets Act) and in EU Member States will affect the activities of the Neutral Host Company.

7 Conclusions

The European Commission has defined a smart city as "a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business" (European Commission, n.d.). The key components of a smart city are inter-operability of systems, city-wide connectivity, and security (Simpson, 2017, p. 4). A 5G network featuring ultra-high speed, super low latency, and massive connectivity is crucial when building a smart city and operating its multiple services and products. The functioning of a smart city requires that a lot of data – and also real time data – is collected from different networks of mobile devices, sensors, connected vehicles, and public places. This helps to better understand the behavioural patterns and demands of residents and respond with appropriate solutions. A smart city ecosystem can provide solutions or solve problems in the fields of traffic and parking, lightning, water consumption, recycling waste, crime prevention and detection, emergency responses, environmental monitoring relating for example to emissions, air pollution levels and providing digital city services.

Building a smart city requires open data and other kinds of data sharing. In addition, citizen engagement and enhanced services for citizens are important (Simpson, 2017, p. 4). However, practical and legal barriers stand in the road to the smart city. A massive amount of data is needed. Its usability increases if it is stored in one place instead of

storing it in silos by many different service providers. Data usability increases when it is stored in a format usable in different systems. Data is usually more valuable if it can be traced to one particular person, because that way it is possible to learn behavioural patterns and adjust and offer services based on that information.

All this raises questions relating to data security and personal data protection. As 5G positioning is capable of measuring accurate locations, the use of smart and connected devices increases the risk to location data privacy. This risk is mitigated with the EU's General Data Protection Regulation and the e-Privacy Directive, which regulate the use of personal data. On the other hand, personal data regulation sets boundary conditions for legitimate use of personal data and can create some restrictions for use of data. Because personal data regulation is quite new, it seems unlikely that it will be changed in the relevant respects, at least in the near future. A flexible interpretation of legitimate interest and public interest as grounds for processing, added to taking data protection requirements into account even at the design state of services will enable development of the smart city and its services. An adequate level of personal data protection and citizens' trust in legal processing of data and data security raise willingness to share data with the Neutral Host (data market place) and take advantage of the many services that service providers in the smart city can make available. Informing data subjects about the purposes of data processing and how and why data is processed, as well as transparency of the functions of the controller, bear an important role in building data subjects' trust.

The requirement of transparency and responsibility also relates to provision of AI-driven products and services. The European regulatory approach to AI aims at balancing between sharing the risks of harm and damage caused by AI on the one hand, and promotion of innovation on the other hand. Operators in the Neutral Host ecosystem developing, deploying, or using AI-based solutions must closely follow the ongoing discussions and be prepared to comply with upcoming adjustments to existing legislation and any AI-specific legal instruments. As far as no special regulation exists, the basic rules and principles of tort law, contract law, and product liability law apply to damage caused by the use of AI.

Telecommunication regulation supports building and operating the 5G connectivity networks that smart city solutions require. Moreover,

cybersecurity and OI regulation help to ensure secure and equal use of 5G networks for end-users. Even though the impact of EU regulation has increased in the telecommunication field, certain country-specific rules need to be paid particular attention when engaging in operative actions in the connectivity platform. For example, decisions on frequency allocation and spectrum licence conditions need to be considered separately for each smart city area. Moreover, the competent authorities for granting spectrum licence permission may differ between Member States. Rules of competition law are also of high importance as running 5G networks may entail more forms of cooperation among actors in the connectivity platform. For example, approval by competition authorities may also be needed for network sharing agreements and joint ventures between the parties involved.

One advantage of a smart city ecosystem is that it supports energy efficiency, the use of green energy and development of more environmentally friendly solutions in traffic. Kera area in the city of Espoo has been planned to become an international example area of the circular economy, with existing rail traffic and 5G technology enabling implementation of IoT and mobility solutions. We believe that in the future the requirements of the smart city for urban planning will be better taken into account, as this will also contribute to other goals considered important in society, such as sustainability and the circular economy.

While EU and national competition law do not pose any fundamental obstacle to the data platform or 5G connectivity aspects of smart cities, the various practices involved in establishing and operating them need to be evaluated carefully by the parties since they are capable of harming competition and can thus require justification. Moreover, some practices that might be involved, such as creation of joint ventures, must be notified to one competition law authority or several authorities for review before they can be implemented. At the moment, uncertainty prevails over how competition authorities and courts will treat some of these practices as no precedents exist in case law or guidance for the novel arrangements concerned (e.g. 5G connectivity offered as a Neutral Host). Moreover, the parties should monitor legislative work under way at EU and national level as that may in the future particularly affect how data platforms can be operated.

In conclusion, the current legislative framework provides a good basis for building a smart city and data marketplace. The most sig-

nificant factor influencing development of the data marketplace is probably personal data protection regulation, which sets the boundary conditions for collection and use of data. To tackle this problem it is important to be aware of regulation and recent interpretation in order to avoid over-cautious conclusions. The restrictions imposed by personal data protection regulation do not apply only to companies operating in Finland, but to all companies offering products and services to consumers in Europe. Similarity of the level of protection can be considered as an advantage, because it makes it easier for companies to offer their products and services for consumers in all EU countries. An adequate level of personal data protection can also become a competitive advantage.

References

Article 29 Data Protection Working Party (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Accessed 27 January 2021).

Austrian Regulatory Authority for Broadcasting and Telecommunications (2018). *Position Paper on Infrastructure Sharing in Mobile Networks*. Available at https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/TKKPositionInfrShare2018.en.html (Accessed 27 January 2021).

BEREC (2018). *Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines.* Available at https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines#:~:text=In%20general%2C%20BEREC%20concludes%20that,the%20views%20of%20many%20stakeholders (Accessed 27 January 2021).

BEREC (2019). *Common Position on Mobile Infrastructure Sharing.* Available at https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/common_approaches_positions/8605-berec-common-position-on-infrastructure-sharing (Accessed 27 January 2021).

BEREC (2020a). *Guidelines on the implementation of the Open Internet Regulation.* Available at https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation (Accessed 27 January 2021).

BEREC (2020b). *Guide to the BEREC 5G Radar and 5G Radar*. Available at https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9721-guide-to-the-berec-5g-radar-and-5g-radar (Accessed 2 February 2021).

Bourreau, M., Hoerning, S. and Maxwell, W. (2020). *Implementing co-investments and network sharing*. Centre on regulation in Europe (CERRE) Telecom Report. Available at https://cerre.eu/publications/telecom-co-investment-network-sharing-study/ (Accessed 27 January 2021).

Bu-Pasha, S. (2020) 'The controller's role in determining 'high-risk' and data protection impact assessment (DPIA) in developing digital smart city', *Information & Communications Technology Law*, 29(3), pp. 391–402.

Campbell, S. (1996). *Green Cities, Growing Cities, Just Cities? Urban planning and the Contradictions of Sustainable Development* [Online]. Journal of the American Planning Association. Available at https://quod.lib.umich.edu/m/mjs/12333712.0001.007?view=text;rgn=main (Accessed 30 December 2020).

City of Espoo. *Kaupunkisuunnittelulautakunnan ehdotus kaupunginhallitukselle asemakaavaksi (Suggestions of the Kera area's local detailed plan that still needs to be accepted)* [Online]. Available at https://www.espoo.fi/fi-FI/Asuminen_ja_ymparisto/Kaavoitus/Asemakaava/Asemakaavoituskohteet/Leppavaara/Kera_130140/Hyvaksyminen (Accessed 23 December 2020).

City of Espoo (2019). *Kera* [Online]. Available at https://www.espoo.fi/kera (Accessed 26 December 2020).

City of Espoo (2020a). *For a sustainable city* [Online]. Available at https://www.espoo.fi/en-US/Housing_and_environment/Districts/Kera/For_a_sustainable_city(189709) (Accessed 26 December 2020).

City of Espoo (2020b). *Sustainable solutions with circular economy* [Online]. Available at https://www.espoo.fi/en-US/Housing_and_environment/Sustainable_development/Sustainable_solutions_with_circular_econ(185317) (Accessed 23 December 2020).

City of Tampere (2020). *Kaavoitusohjelma 2020–2024 (Planning Program 2020–2024)* [Online]. Available at https://tampere.cloudnc.fi/download/noname/%7Bc6b78824-1f5a-4bb9-bb43-1e92847a94ec%7D/3858725 (Accessed 25 December 2020).

Edwards, L. (2016). 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective', *European Data Protection Law Review*, 2(1), pp. 28–58.

European 5G Observatory (2020). *5G Observatory Quarterly Report 9. Up to September 2020*. Available at http://5gobservatory.eu/wp-content/uploads/2020/10/90013-5G-Observatory-Quarterly-report-9-V2.pdf (Accessed 1 February 2021).

European Commission. *Smart cities* [Online]. Available at https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en (Accessed 23 February 2021).

European Commission (2017). *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy.* Accompanying the document Communication Building a European data economy. Available at https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy (Accessed 25 January 2021).

European Commission (2018a). *Artificial Intelligence for Europe*. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN (Accessed 17 December 2020).

European Commission (2018b). *Coordinated Plan on Artificial Intelligence*. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0795 (Accessed 18 December 2020).

European Commission (2020a). *Proposal for an ePrivacy Regulation* [Online]. Shaping Europe's digital future. Policy. Available at https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (Accessed 27 January 2021).

European Commission (2020b). *White Paper on Artificial Intelligence – A European approach to excellence and trust*. Available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (Accessed 16 December 2020).

European Commission (2020c). *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en (Accessed 16 December 2020).

European Commission (2020d). *A European strategy for data*. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN (Accessed 27 January 2021).

European Commission (2020e). *Sustainable corporate governance. Inception impact assessment – Ares(2020)403403.* Published initiatives. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12548-Sustainable-corporate-governance (Accessed 30 December 2020).

European Commission (2020f). *New Competition Tool ('NCT'). Inception impact assessment – Ares(2020)2877634*. Published initiatives. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12416-New-competition-tool (Accessed 17 January 2021).

European Data Protection Board (2020a). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0*. Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (Accessed 27 January 2021).

European Data Protection Board (2020b). *Guidelines 3/2019 on processing of personal data through video-devices. Version 2.0*. Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (Accessed 24 January 2021). European Data Protection Board and European Data Protection Supervisor (2021). *EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on the European data governance (Data Governance Act)*. Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-edps_joint_opinion_dga_en.pdf (Accessed 16 March 2021).

European Parliament (2020a). *Framework of ethical aspects of artificial intelligence, robotics and related technologies*. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. Available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf (Accessed 16 December 2020).

European Parliament (2020b). *Civil liability regime for artificial intelligence*. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence. Available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf (Accessed 16 December 2020).

European Parliament (2020c). *Intellectual property rights for the development of artificial intelligence technologies*. European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies. Available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf (Accessed 16 December 2020).

Expert Group on Liability and New Technologies – New Technologies Formation (2019). *Liability for Artificial Intelligence and other emerging digital technologies*. Available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608 (5 February 2021).

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (2019). Case C-40/17. ECLI:EU:C: 2019:629.

Finnish Competition and Consumer Authority (2015). Decision dnro 438/14.00.00/2014. Available at https://www.kkv.fi/globalassets/kkv-suomi/ratkaisut-aloitteet-lausunnot/ratkaisut/kilpailuasiat/2015/kielto–sitoumus–ja-toimitusvelvoiteratkaisut/r-2014-00-0438.pdf (Accessed 27 January 2021).

Finnish Government. *Hanke: Kestävän kehityksen koordinointiverkosto* (*Project: Sustainable Development Coordination Network)* [Online]. Available at https://vnk.fi/hanke?tunnus=VNK026:00/2015 https://ym.fi/hankesivu?tunnus=YM034:00/2017 (Accessed 30 December 2020).

FRA (European Union Agency for Fundamental Rights) (2020). *Getting the future right – Artificial Intelligence and fundamental rights.* Luxembourg: Publications Office of the European Union. Available at https://eu2020-bmjv-european-way-on-ai.de/storage/documents/FRA_AI_Report.pdf?fbclid=IwAR1Oc_slMYL6ybv5o6jrdGGjHQJMGFiFVBo7aLQXG3s_ik4FXlyeMwmCrbI (Accessed 17 December 2020).

Gervais, D. (2019). 'Exploring the interface between big data and intellectual property', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* 10(1), pp. 3–19.

High-Level Expert Group on Artificial Intelligence (2019a). *A definition of AI: Main capabilities and scientific disciplines*. Available at https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (Accessed 18 December 2020).

High-Level Expert Group on Artificial Intelligence (2019b). *Ethics guidelines for trustworthy AI*. Available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (Accessed 18 December 2020).

ICO (2017). *Legitimate interests* [Online]. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (Accessed 1 January 2021).

KPMG (2020). *The Time Has Come: The KPMG Survey of Sustainability Reporting 2020*. Available at https://home.kpmg/content/dam/kpmg/fi/pdf/12/KPMG_Time_has_come_External_presentation_pdf.pdf (Accessed 30 December 2020).

Lohan, E.S., Alén-Savikko, A., Chen, L., Järvinen, K., Leppäkoski, H., Kuusniemi, H. and Korpisaari, P. (2018). '5G Positioning: Security and Privacy Aspects' in Liyanage, M., Ahmad, I., Abro, A.B., Gurtov, A. and Ylianttila, M. (eds.), *A Comprehensive Guide to 5G Security*. Wiley, pp. 281–320.

Ministry of Economic Affairs and Employment in Finland. *Key Guidelines on Corporate Social Responsibility* [Online]. Available at https://tem.fi/en/key-guidelines-on-csr (Accessed 19 December 2020).

Ministry of the Environment. *MRL-kokonaisuudistus (Reform of the Land Use and Building Act)* [Online]. Available at https://ym.fi/hankesivu?tunnus=YM014:00/2018 (Accessed 30 December 2020).

Ministry of Justice (2020). *Lausuntopyyntö: Osakeyhtiölain toimivuus ja muutostarpeet (Request for an opinion: Need for changes in Companies Liability Act)* [Online]. Available at https://api.hankeikkuna.fi/asiakirjat/18611670-d9a0-4e78-ab3f-abc65b0ef02c/ab01fd6d-48c8-4e5f-b540-137115ab4592/LAUSUNTOPYYNTO_20201021091349.PDF (Accessed 30 December 2020).

Nations World Commission on Environment and Development (1987). *Our Common Future Report*. Available at https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf (Accessed 25 December 2020).

Netherlands Authority for Consumers and Markets (2019). *ACM to draw up guidelines for the sharing of telecom infrastructure* [Online]. Available at https://www.acm.nl/en/publications/acm-draw-guidelines-sharing-telecom-infrastructure (Accessed 27 January 2021).

NIS Cooperation Group (2020). *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures*. CG Publication 01/2020. Available at https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (Accessed 27 January 2021).

OECD (2011). *OECD Guidelines for Multinational Enterprises*. OECD Publishing 2011. Available at http://mneguidelines.oecd.org/guidelines/ (Accessed 19 December 2020).

OECD (2015). *Wireless Market Structures and Network Sharing.* OECD Digital Economy Papers, No. 243. OECD Publishing 2014. Available at https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2014)2/FINAL&docLanguage=En (Accessed 1 February 2021).

Pihlajarinne, T. and Ballardini, R.M. (2019). 'Owning Data via Intellectual Property Rights: Reality or Chimera?' in Ballardini, R.M. – Kuoppamäki, P., and Pitkänen, O. (eds.) *Regulating Industrial Internet Through IPR, Data Protection and Competition Law*. The Netherlands: Kluwer Law International B.V., pp. 115–133.

Ristaniemi, M. (2020). 'Yritysvastuun normeista', *Edilex-artikkelit*. Available at https://www.edilex.fi/artikkelit/21345.pdf (Accessed 23 December 2020).

Simpson, P. (2017) *Smart Cities: understanding the challenges and opportunities* [Online]. Philips and SmartCitiesWorld Report. Available at https://smartcitiesworld.net/AcuCustom/Sitename/DAM/012/Understanding_the_Challenges_and_Opportunities_of_Smart_Citi.pdf (Accessed 23 February 2021).

Telenor Magyarország Zrt. v. Nemzeti Média- **és** Hírközlési Hatóság Elnöke (2020). Joined Cases C807/18 and C39/19. ECLI:EU:C:2020:708. (Telenor Hungary)

Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta (2018). Case C-25/17. ECLI:EU:C:2018:551.

TNO (2018). *5G and Net Neutrality: a functional analysis to feed the policy discussion* [Online]. Available at https://www.tno.nl/en/about-tno/news/2018/4/5g-net-neutrality-a-tno-study/#:~:text=TNO%20has%20made%20a%20detailed,than%20the%20current%204G%20networks (Accessed 27 January 2021).

De la Torre, L. (2019) *What is a 'Data Protection Impact Assessment' (DPIA) under EU Law?* [Online] Golden Data. Available at https://medium.com/golden-data/what-is-a-data-protection-impact-assessment-dpia-under-eu-law-644e46ce9b62 (Accessed 22 February 2021).

Traficom (2019). *Digital services and infrastructure* [Online]. Available at https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/digital-services-and-infrastructure (Accessed 27 January 2021).

UN (2015). *Transforming our world: the 2030 Agenda for Sustainable Development* [Online]. Available at https://sdgs.un.org/2030agenda (Accessed 19 December 2020).

UN Global Compact (2019). *Guide for General Counsel on Corporate Sustainability Version 2.0*. Available at https://www.unglobalcompact.org/library/5722 (Accessed 19 December 2020).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (2018) Case C-210/16. ECLI:EU:C:2018:388.

Vodafone Italia / TIM / Inwit JV (2020). European Commission Merger Case M.9674. Available at https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_9674 (Accessed 27 January 2021).

Voigt, P. and von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer International Publishing AG.

Wray, S. (2020). *What does the EU's Data Governance Act mean for smart cities?* [Online] Cities Today. Available at https://cities-today.com/what-does-the-eus-data-governance-act-mean-for-smart-cities/ (Accessed 27 January 2021).

Zech, H. (2021). 'Liability for AI: public policy considerations', *ERA Forum*. Available at https://doi.org/10.1007/s12027-020-00648-0 (Accessed 27 January 2021).