Advances in Social Science, Education and Humanities Research, volume 441
6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)

Leading Approaches to the Artificial Intelligence in the Transport Environment of the Smart City

Arseniy Bimbinov
Kutafin Moscow State Law University (MSAL)
Sadovaya-Kudrinskaya Str., 9, 125993 Moscow
Russian Federation
e-mail: bimbinov@yandex.ru

Abstract This paper is dedicated to identifying the most likely and dangerous threats to humans in the transport environment of a smart city. The research was carried out through analyzing the published plans for the development of the transport environment of the smart city in the Russian Federation and promising innovations in this area abroad. In each of the areas, we identified the most likely scenarios of harming public relations which we subsequently put under the legal assessment.
Our results demonstrate that in relation to one of the possible threats (harm during operation of unmanned vehicles), the current criminal law is powerless. It is determined that the regulation of issues related to "intelligent" technologies, including regarding the harm they cause, should be based on certain general provisions that are universal in nature.

Keywords: *artificial intelligence, transport environment, smart cities, leadership*

1 Introduction

Modern society exists in an amazing time. Today, each of its members can observe the changes taking place in all spheres of human activity, without being distracted from their usual way of life. Just a couple of decades ago, it was hard to imagine that wireless communications, the ubiquitous high-speed Internet, digital broadcasting and individually selected information space will firmly enter our life and become its integral part. Every year, digital technologies improve, become more accessible, their scope is growing. The search abilities of the Internet, self-taught equipment, and artificial intelligence no longer cause the previous enthusiastic exclamations. Entire industries and regions with their functional complexes, including transport infrastructure, are being digitalized. Digital flight monitoring, optimization of multimodal freight transportation with electronic freight documents, harmonization of schedules for various types of passenger transport, big data from the transport industry, unmanned vehicles, smart roads and a smart city - all these are the prospects for the coming years.

The concept of integration of information and communication technologies and the Internet of things for city management (smart city) is aimed at improving the quality of life with the help of computer technology, increasing the efficiency of services and meeting the needs of citizens. Through the use of digital technologies integrated into the urban environment, data from urban residents and their devices are collected and analyzed. The information collected is used to quickly solve urban problems, increase productivity and interactivity of city services, reduce costs and resource consumption, improve communication between city residents and the state. The main areas covered by the smart city concept are public services, energy conservation, healthcare, water management, waste management and urban transport network management (Paskaleva 2009).

Managing the urban transport network of a smart city is a well-functioning mechanism that uses innovative developments to regulate traffic flows, unload roads, ensure uninterrupted movement of all types of transport and ensure public safety (Strielkowski et al. 2020). Therefore, for example, the main directions of the development of the transport environment of the “Smart City of Moscow” are: the implementation of the concept of “Mobility as a Service” (involves real-time selection of optimal route parameters, travel time, cost, level of comfort and environmental effect), creating an online personified city -service of intellectual mobility, the creation of road transport infrastructure for the use of unmanned vehicles, the launch of unmanned vehicles, the use of exclusively electronic clean electric public transport, improving the safety, comfort and environmental friendliness of the transport system using digital technology, reducing the average time of a city trip due to the intelligent transport system and digital services, increasing the efficiency of traffic management and reducing road traffic accidents due to big data analytics and others digital technologies, synchronized harmonized development of the transport infrastructure of the city of Moscow and Moscow th area, the rejection of the use of personal vehicles (Mos.ru 2020).

Such transformations as a whole will have a very positive effect. However, like any other large-scale changes in the life of society, they will have negative results. It is not possible to predict all the negative

consequences of implementing the concept of a smart city, but today it is safe to say that the negative consequences will primarily affect the socio-economic sphere (labor market, competition, etc.) and security issues. Socio-economic consequences will not immediately appear (see e.g. Strielkowski 2019). A prudent government policy in the field of digital development presupposes a transition period during which they will try to minimize the negative socio-economic consequences. As for security issues, certain negative consequences in this area are already showing, and many will appear in the near future. The expansion of the use of digital technologies in the transport environment entails an increase in the possibilities of dangerous, including criminal and other illegal activities. New opportunities (for collecting and using protected information, withdrawing and transferring funds, for automatic process control, etc.) are already being used in the criminal environment. The proportion of theft and fraud committed using digital technology will increase. Modern developments take the mechanism of harm to a new plane. The question of liability for harm caused by uncontrolled human technology remains open. In such circumstances, the law, as a universal regulator, should already have the means to respond to such cases and meet new security challenges. Meanwhile, the current criminal law toolkit is not relevant, and the legislative initiatives discussed are not sufficient (Lukashevich 2019; or Fokin and Ryazanov 2018). The legal regulation of the development of digital technologies, including criminal law, unfortunately, with a margin lags behind reality, as it does not meet current challenges, not to mention the upcoming ones. If the situation is not corrected, not acted in advance, there will be a threat of loss of control over the situation and putting security and law and order issues dependent on the capabilities of certain technologies and their developers. In this regard, it is necessary to conduct a study on the identification of the main threats to humans in the transport environment of a smart city and their criminal law assessment.

This paper aims at identifying the most possible and potentially dangerous threats to humans in the transport environment of a smart city and their legal assessment. In order to do this, the following issues need to be investigated: First, the methods for searching for vulnerabilities in the transport environment of a smart city should be defined. Second, all potential threats to humans in the transport environment of a smart city should be classified. Third, an analysis of the possible consequences of the identified shortcomings of the transport environment of the smart city should be carried out. Finally, legal assessment of identified risks from the perspective of the current criminal law needs to be done.

2. Literature review

Until recently, serious legal research in the field of the development of digital technologies and their impact on security has not been conducted in Russia. However, the state policy to intensify digital development and grant programs of the Government of the Russian Federation and scientific foundations have changed the situation. Today, there are works devoted to both the impact on the security of digital technologies in general, and the issues of security of the digital transport environment.

A research team led by Waipana and Egorova reflected the results of a study of the features of the legal regulation of economic relations in the context of the development of the digital economy. The authors paid special attention to special legal models for protecting relations based on the use of digital technologies, including issues of cybernetic and information security (see Belitskaya et al. 2019).

Selivanov et al. (2017) substantiated the need to deploy a strategic management system, create powerful intellectual support for the national system, economic security and strategic management as the main tool to neutralize and prevent potential negative effects in the transition to the sixth technological structure under changing competitive conditions, new challenges and threats to economic security.

Antonova et al. (2019) attempted to develop a legal concept for robotics based on the following key points: firstly, it should reflect the processes of robotization in the general context of the legal regulation of socio-economic processes and be implemented in stages; secondly, it is advisable to develop concepts in this area, reflecting both general legal and sectoral legal concepts, as well as combined with special ones; thirdly, robotics in the focus of law involves the formation of new statuses of subjects of legal relations, including modes of joint and autonomous action of a system of robots; fourthly, it is necessary to take into account the specifics of legal institutions in conditions of robotization, especially competencies, decisions, ways of relationships, procedures of activity; fifthly, it is necessary to anticipate both the modification and narrowing of certain objects and methods of legal regulation, and the emergence of new legal phenomena. Arkhipov et al. (2019) considered a significant layer of legal issues that arise in society in connection with the active development of two relatively new technologies: robotics and artificial intelligence.

The security issues of the digital transport environment are mainly devoted to the study of the problems of human interaction and “intelligent” technologies. Kuteynikov et al. (2019) studied various legal approaches to the regulation of public relations related to the interaction of a person with technical means (physical and virtual entities) that can make decisions independently of a person. The authors concluded that technical means acquire a sign of autonomy only when they are under the control of an artificial cognitive system (artificial intelligence).

Korobeev and Chuchaev (2019) focuses on the dangers posed by unmanned vehicles for personal, property and other relationships in connection with traffic accidents and the resulting moral and legal problems. The team proposed a roadmap, firstly, to address gaps in legislation (for example, those found in civil and administrative law), secondly, to develop safety rules for the operation and operation of unmanned vehicles, and thirdly, to design a criminal law liability for damage caused by the drone.

Khisamova and Begishev (2019) investigated the issues of criminal legal assessment of the behavior of artificial intelligence. Scientists insist on the need to create a system of criminal law measures to counter crimes committed with the use of artificial intelligence, in connection with the unresolved issue of responsibility for the actions of artificial intelligence, which has the ability to self-study, which decided to commit actions / inaction that qualify as a crime.

In a joint Russian-American study, Neznamov and Smith (2019) highlighted the problems of responsibility for the actions (inaction) of robots from the standpoint of two law and order - the United States and Russia. The authors, referring to the provisions of national laws, demonstrate the existing approaches to the problem of responsibility in law, in the theory of law and law enforcement acts.

In the Anglo-American doctrine, studies on the search for vulnerabilities of human-artificial intelligence interfaces have been carried out for a long time, however, they are mainly devoted to military unmanned vehicles and unmanned aerial vehicles (Hubbard 2014; Beard 2018).

In Germany, a large number of scientific works are related to the impact on the urban environment of unmanned aerial vehicles. There are articles on the regulation of the use of self-propelled (unmanned) land vehicles (autonomes Landfahrzeug). Of particular interest are studies of ethical decisions in road traffic accident scenarios involving unmanned vehicles. A team of scientists from the University of Osnabruck used immersive virtual reality to evaluate ethical behavior in simulated traffic scenarios and used the collected data to train and evaluate a number of decision models of artificial vehicle intelligence (Sütfeld et al. 2017).

Chinese researchers also focus on ethical issues. The authors described the main areas of application for driverless cars in China and abroad, summarized the technical difficulties and problems faced by autonomous vehicles, and suggested possible solutions and scenarios for the use of autonomous vehicles in the future (Xu and Fan 2019).

In the study of the Greek team, an approach was proposed to determine the index of the city's readiness for autonomous vehicles. The risk management process for smart port cities is described with an emphasis on the coordination of complex port subsystems and coastal areas. The process is based on risk analysis of potential hazards in order to better understand their nature and the need for prevention strategies (Golias et al. 2019).

Moreover, many scientific papers devoted to the problems of the transport environment of smart cities have been prepared by joint international teams. The US-Australian study provides examples of security, privacy, and ethical issues with unmanned vehicles, which are a major concern for the future of smart cars (Mohammed et al. 2014).

A Spanish-Chilean group of scientists made an attempt to describe the macroscopic effects of the interaction of modern mobility and the urban environment for present and future cities (Medina-Tapia and Robusté 2018).

Research is also being carried out in neighboring countries. Savenok (2018) in his work substantiates the need to improve individual criminal law standards, as well as develop a state concept for the development of robotics and artificial intelligence systems in the Republic of Belarus, which should become a strategic area of activity for the coming years.

3. Research methods

It seems that the identification of potential threats to humans in the transport environment of a smart city is possible only by studying the directions of development of digital technologies of this concept and modeling the negative consequences that are allowed.

Thus, our study will be carried out by analyzing the published plans for the development of the transport environment of the smart city in Russia and promising directions in this area abroad. In each of the areas the most likely scenarios of harming public relations will be identified, which will be given a legal assessment.

Our paper suggests the use of private methods: legal analytics, legislative technology, legal comparative studies, and expert assessment methods.

4. Development of the transport environment of a smart city in Russia

The basis for planning activities for the implementation, including the concept of a smart city, is the roadmap of the Avtonet National Technological Initiative (Appendix No. 2 to the minutes of the meeting of the Presidium of the Presidential Council on Economic Modernization and Innovative Development of Russia dated April 24, 2018, No. 1). The scope of this roadmap lies in the plane of transport and logistics and navigation and telecommunications

infrastructure and has a direct impact on other industries and the country's economy as a whole, being essentially the driver of economic growth at present.

The specific steps for the implementation of digital technologies in the urban transport environment are defined by the standard "Basic and additional requirements for smart cities (the Smart City standard)", approved by the Ministry of Construction of Russia. This standard, among other things, assumes:

1. The introduction of automatic photo and video recording systems using high-definition security cameras into the transport infrastructure. It is assumed that such means of video surveillance will be scanned, including by the faces of road users (the developers claim that this will allow them to refuse tickets and pay for the trip by automatically debiting funds from the electronic wallet tied to the passenger). This is probably why the expected effect is indicated by the access of law enforcement agencies to data from the system for the speedy implementation of operational-search measures.

Such prospects make us think about threats to privacy and other constitutional human rights and freedoms. The rapidly growing number of interconnected monitoring and recording devices installed in cities multiplies the amount of information about citizens. The scope of the information collected and used is huge: from determining the location and route of movement to ending with the establishment of social ties and behaviors. Such processes largely occur without the knowledge of the affected persons and without their informed consent. Romashov (2019) writes that strengthening the analytical potential of data-based technologies continues to grow exponentially. Big data analysis methods and artificial intelligence expand the ability of states and companies to obtain accurate information about people's lives, draw conclusions about their physical and mental characteristics and create detailed personal files. The result is an environment that creates threats to people and societies that are hard to overestimate.

For example, in recent years there have been huge data breaches, as a result of which affected individuals have become victims of identity theft and the disclosure of deeply personal information (Romashov 2019). Such information may be unlawfully used in electoral processes, in the provision of financial services, in insurance, and so on. In addition, possible attempts by law enforcement agencies to identify persons posing a potential security risk in the context of predicting criminal behavior are a violation of constitutional rights and border on discrimination. As the European Court of Human Rights stated in the case of Roman Zakharov v. Russia: "a covert surveillance system to protect national security can diminish or even destroy democratic values under the pretext of protecting them" (ECHR 2015).

2. The introduction of a unified system of payment for travel in public transport with the possibility of non-cash payment methods. In Moscow, this system has already been introduced to a certain extent. The threats to operating such a system are about the same as in any other area using non-cash payment methods (Arkhipov 2018).

3. Development of technologies that ensure the movement of unmanned vehicles on highways, as well as the introduction of intelligent transport systems on public roads, including, inter alia, the provision of unmanned vehicles. In addition, until March 1, 2022, an experiment will be conducted on the pilot operation of highly automated vehicles on public roads. The main danger of the innovations presented is the possibility of innocent harm in road traffic accidents. Bubnovskaya (2019) writes that harm can be caused by various factors, among them: cyberattacks, system errors, non-updating of a program, situations when the system chose an option that the driver would never have chosen when the system for this section of the terrain was out of date, when the user misinterpreted the recommendations of the system (Bubnovskaya 2019).

In the framework of this experiment, in the absence of guilty actions of other road users, liability for road traffic and other incidents that occurred with the participation of a highly automated vehicle is borne by its owner - a legal entity. Outside of the experiment, the question is open. The reason for this is the lack of a normative legal basis for regulating the conditions and procedure for using "intelligent" technologies, including transport robots.

5. Development of the transport environment of a smart city in other countries

A number of countries have already made an attempt to legislatively regulate issues related to the production and operation of unmanned vehicles and liability for causing damage to them. So, at the National Conference of Commissioners for the Unification of the Legislation of the United States (October 26-28, 2018) a draft Act on highly automated vehicles was developed. This project makes significant changes to the sections on registration of automated vehicles and automated driving operators. Also in the United States, the Automated Moving Systems Safety Concept 2.0 Act is in force, which defines 12 safety criteria for operating highly automated vehicles.

The problem of regulation of unmanned vehicles and automated driving is also discussed at the international level. Thence, from March 19 to March 23, 2018, a session of the working group on traffic safety of the UN Inland Transport Committee was held in Geneva. The session discussed the wording of the resolution on the introduction of highly and fully automated vehicles in traffic conditions, which outlines recommendations for users of automated driving systems. At the same time, the current trend in the legislation of economically developed countries is the responsibility on the driver for driving a vehicle even with a relatively high degree of automation, which implies the duty of the driver to maintain control over the road situation and over the vehicle. Cases of vehicle operation in the absence of a driver are also characterized by legal uncertainty.

The concept of a smart city in foreign countries also involves the widespread introduction of objective observation tools for data collection, their in-depth analysis and use, including for preventive purposes. Scientists note that a further increase in the way people observe human beings by the authorities is combined with a panopticon-like concept of continuous enforcement and introduces a level of individualistic paternalism when citizens are considered unable to voluntarily comply with laws and other rules of human society (Finch and Omer 2014).

Another problem in the development of the transport environment of a smart city, according to foreign researchers, is, oddly enough, the over-digitalization of urban infrastructure, including sources of increased danger (Graham and Marvin 1996). Illegal access to process control in the developed transport environment of a smart city can lead to dangerous consequences, the scale of which is difficult to overestimate.

6. Conclusions

Thus, the following potential threats to humans in the transport environment of a smart city can be distinguished:

- The threat of discrimination and violation of the person’s privacy;
- the threat of property damage when using electronic commerce;
- the threat of physical and property damage during the operation of unmanned vehicles;
- the threat of causing any harm with unauthorized access to the "intellectual" technologies of a smart city.

All of the listed threats, except one, if implemented, can receive a criminal legal assessment according to the norms of the current legislation. Thus, discrimination and violation of privacy invoke liability under Articles 136 and 137 of the Criminal Code of the Russian Federation. Causing property damage is qualified, as a rule, in accordance with the norms of Chapter 21 of the Criminal Code of the Russian Federation. Responsibility for unauthorized access to technology and the use of malicious computer programs is provided for in Articles 272-273 of the Criminal Code of the Russian Federation. However, the application of these standards, even in situations not burdened by new digital technologies, causes problems. Further improvement of the legislative description and practice of applying these standards should be carried out taking into account new and promising technological realities.

The current legislation does not allow criminal prosecution of a person for damage caused by an unmanned vehicle that independently decided to commit a dangerous maneuver. The Criminal Code of the Russian Federation does not contain norms in this regard, therefore, suggestions are made to supplement the law with norms on the liability of the manufacturer, developer or operator (driver) of the transport robot-violator. It seems that such criminal law changes should not be rushed. Regulation of issues related to “intelligent” technologies, including regarding the harm they cause, should be based on certain general provisions that are universal in nature. Transport, robotics and digital technology in general are globalist categories. The process of their development, production and implementation, even in a single country, is always carried out taking into account the existing positive foreign experience. Further development of digital technologies, including unmanned vehicles, is likely to also be carried out through a close interweaving of knowledge-based industries based on transnationalization. Therefore, the general provisions on digital technologies and artificial intelligence should be enshrined in supranational legislation in the form of principles, on the basis of which detailed regulation of the features of the use of "intelligent technologies" in national jurisdictions is possible.

Acknowledgments

This research was supported by the Russian Federal Property Fund by agreement No. 19-29-06069 mk.

References

Antonova NV, Balkhaeva SB, Gaunova ZhA, The legal concept of robotics, 1st edn. (Moscow, Prospect, 2019), 240 p.

Arkhipov AV (2018) Responsibility for the theft of non-cash and electronic money: legislative novels. Criminal Law 3: 4-9

Arkhipov VV, Bakumenko VV, Volynets A.D, Robotics regulation: an introduction to Robo-Law. Legal aspects of the development of robotics and artificial intelligence technologies, 1st edn. (Moscow, Infotropic Media, 2019), 232 p.

Beard JM (2018) The Principle of Proportionality in an Era of High Technology. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3119384 Accessed on 22 Mar 2020

Belitskaya AV, Belykh VS, Belyaeva OA, Legal regulation of economic relations in modern conditions of development of the digital economy, 1st edn. (Moscow, Justicinform, 2019), 376 p.

Bubnovskaya TA (2019) Civil liability when using unmanned vehicles. Transport Law 3: 6-9

Finch K, Omer T (2014) "Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town". Fordham Urban Law Journal 41:1581. https://ir.lawnet.fordham.edu/ulj/vol41/iss5/4 Accessed on 20 Mar 2020

Fokin MS, Ryazanov NS (2018) Actual problems of the criminal law regulation of the unlawful use of unmanned mobile vehicles. Actual problems of Russian law 1: 103-110 doi 10.17803 / 1994-1471.2018.86.1.103-110

Golias M, Dedes G, Douligeris C, Mishra S (2019) Challenges, Risks and Opportunities for Connected Vehicle Services in Smart Cities and Communities. IFAC-PapersOnLine 51 (34): 139-144 doi: 10.1016/j.ifacol.2019.01.056.

Graham S, Marvin S, Telecommunications and the city: electronic spaces, urban place, 1st edn (London: Routledge, 1996), 456 p.

Hubbard PF (2014) “Sophisticated Robots”: Balancing Liability, Regulation, and Innovation. Florida Law Review 66(1803). http://scholarship.law.ufl.edu/flr/vol66/iss5/1 Accessed on 19 Mar 2020

Khisamova ZI, Begishev IR (2019) Criminal liability and artificial intelligence: theoretical and applied aspects. All-Russian Criminological Journal 13(4): 564-574. doi: 10.17150 / 2500-4255.2019.13 (4) .564-574

Korobeev AI, Chuchaev AI (2019) Unmanned vehicles: new challenges to public safety. Lex Russia 2: 9-28 doi: 10.17803/1729-5920.2019.147.2.009-028

Kuteynikov DL, Izhaev OA, Lebedev VA, Zenin SS (2019) Regulation of human interaction with autonomous technical means: discussion of legal regimes. Lex Russia 9: 85-95. doi 10.17803 / 1729-5920.2019.154.9.085-095

Lukashevich SV (2019) Unmanned vehicle: a paradigm shift as a result of the digitalization of the economy. Transport law 3: 3-5

Medina-Tapia M, Robusté F (2018) Exploring paradigm shift impacts in urban mobility: Autonomous Vehicles and Smart Cities. Transportation Research Procedia 33: 203-210 doi: 10.1016/j.trpro.2018.10.093.

Mohammed F, Idries A, Mohamed N, Al-Jaroodi J, Jawhar I (2014) UAVs for smart cities: Opportunities and challenges. 267-273 doi 10.1109/ICUAS.2014.6842265.

Mos.ru (2020) Development directions of the Smart City of Moscow. Official site of the Mayor of Moscow. https://www.mos.ru/2030/n/n3/ Accessed on 29 Mar 2020

Neznamov A., Smith BU (2019) The robot is not to blame! A view from Russia and the USA on the problem of liability for damage caused by robots. Law 5:135-156

Paskaleva KA (2009) Enabling the smart city: the progress of city e-governance in Europe. International Journal of Innovation and Regional Development 1(4): 405-422 doi: 10.1504/ijird.2009.022730

Romashov PA (2019) On the issue of the right to privacy in the digital age. Perm legal almanac. Annual scientific journal 1: 103-118

Savenok AL (2018) Damage by an unmanned vehicle: qualification issues. Bulletin of the Academy of the Ministry of Internal Affairs of the Republic of Belarus 2(36): 153-156.

Selivanov A.I., Starovoitov V.G., Troshin D.V. (2017) Economic security in the transition to the sixth technological order: statement of the problem. Business Security 6: 10-16

Strielkowski W Social impacts of smart grids: the future of the smart grids and energy market design, 1st edn. (London: Elsevier, 2019), 342 p.

Strielkowski W, Veinbender T, Tvaronavičienė M, Lace N (2020) Economic efficiency and energy security of smart cities. Economic Research-Ekonomska Istraživanja 33(1):788-803. doi: 10.1080/1331677X.2020.1734854

Sütfeld L, Gast R, König P, Pipa G (2017) Using Virtual Reality to Assess Ethical Decisions in Road Traffic Scenarios: Applicability of Value-of-Life-Based Models and Influences of Time Pressure. Frontiers in Behavioral Neuroscience. doi: 10.3389/fnbeh.2017.00122.

Xu X, Fan CK (2019) Autonomous vehicles, risk perceptions and insurance demand: An individual survey in China. Transportation research part A: policy and practice 124:549-556. doi: 10.1016/j.tra.2018.04.009.