Technological Considerations on the Legal Regulation in the Use of Robotic Security Assistants

Dobromira Bankova [1] and Vladimir Dimitrov [1]

[1] *University of Sofia "St. Kliment Ohridski", Faculty of Mathematics and Informatics, 5 James Bourchier blvd., Sofia, 1164, Bulgaria*

Abstract

Modern technological developments allow the use of technologies in the field of advanced robots, automated assistants and artificial intelligence, which permits physical movement of machines based on autonomous solutions through environmental monitoring both for production purposes, as well as for services provision. The European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [1], classifies the types of robots in terms of the services they provide as care robots, medical robots, etc. This paper aims to explore the use of such autonomous solutions, referred to as service robots, in the field of security service provision in urban environments in terms of technological features that influence or determine existing legal regulation. An attempt is made to model their technical characteristics at a high level, with the idea of a more formalized, and technology oriented treatment. The combination of these technological and legal considerations provides accordingly the frame of the potential need of change, actualization and further and build on existing regulations.

Keywords

Service robots, legal regulation, security activity

1. Introduction

The legal regulation of the use of robots for the provision of services within the framework of private law relations constitutes a challenge for our national legal system, since at present, the regulation, insofar as it exists, is related to a specific type of narrowly subject-specific public relations – for example, in relation to the acquisition of specialties in the field of robotics, or to the provision of health services through the use of robots as part of the general treatment structure.

Information Systems & Grid Technologies: Fifteenth International Conference ISGT'2022, May 27–28, 2022, Sofia, Bulgaria
EMAIL: dobromirabankova@gmail.com (D. Bankova); cht@fmi.uni-sofia.bg (V. Dimitrov
ORCID: 0000-0002-9261-2842 (D. Bankova); 0000-0002-7441-253X (V. Dimitrov)

At the level of European regulation there is also currently no unified system. The main documents are related to the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [1] European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, (2020/2014(INL) [2], and European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework for ethical aspects of artificial intelligence, robotics and related technologies [3].

2. Definitions and classification

In the context of the relations under consideration, the basic concepts and possible classifications relevant to regimes of legal regulations are defined.

The robotic systems, which serve as a basic, high-level model for the study of the respective technical characteristics and technological specifics is distinguished by the so-called theory for intelligent agents and their environment (see Figure 1). The agent, in turn, is understood as a robot that explores the environment through sensors (cameras, infrared rays, etc.) and acts/influences the environment through actuators (different motors). The agent has a set program (task), which is a consequence of its function [4, 5, 6].

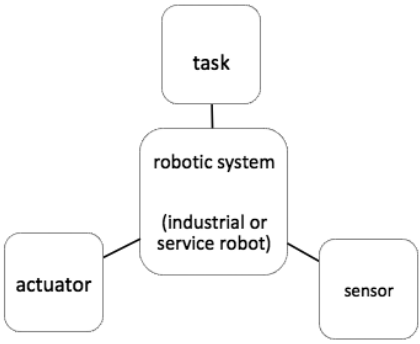

Figure 1: High-level robotic system model

In the studied robotic systems, the accepted definitions for service robots are used. We use the definition of service robots which is based on the concept of industrial robot described in standard ISO 8373: 2012 (International Organization for Standardization [ISO], 2012) [7] and accepted as an appropriate classification in the European Commission's JRC Working Paper on Labor, Education and Technology 2020/14, in particular Sostero, M., Automation and Robots in

Services: Review of Data and Taxonomys, Seville: European Commission, 2020, JRC121893H [8].

First of all, it is a robot defined as a Controllable / Actuated mechanism, programmable in two or more axes with a degree of autonomy (i.e. the ability to perform planned tasks based on the current state and feeling, without human intervention), moving in an environment in order to perform planned tasks. Second, service robots are defined by the tasks they perform and the constraint of industrial robots, such as a robot that performs useful tasks for humans or equipment, with the exception of industrial automation applications that are non-exhaustive linked to production, inspection, packaging and assembly. Also known classification is related to the characteristics of intelligent robots defining them by the signs of autonomy, adaptability, self-learning, the presence of physical media (insignificant), lack of life as a biological concept[2] and the definition given by art 4 of European Parliament resolution of 20 October 2020 (2020/2012(INL) about 'robotics' – technologies that enable automatically controlled, reprogrammable, multi-purpose machines to perform actions in the physical world traditionally performed or initiated by human beings, including by way of artificial intelligence or related technologies.

This study aims to explore the legal regulations conditioned by the technical characteristics and the tasks set for a service robot. Especially when the task set is in the application of private security activities. It should be taken under consideration that there is a national legal framework, a specific law – Private Security Business Act, Promulgated, SG No. 10/30.01.2018, that identifies the subject field of the covered public relations in two main directions [10]:

- protection/prevention from unlawful encroachments on the person, respectively on the health and life of the person, and
- protection/prevention from unlawful encroachments on property.

With regard to property, the law defines various aspects such as protection of the property of individuals or legal entities, incl. agricultural property, and self-protection, understood as parameterization of the activity as protection of specific real estate and / or movables in the first case and as real estate and movable property located in it, in the second case.

The types of security activities, as well as self-protection of property are listed exhaustively and may include:

- the monitoring post as a stationary security patrol,
- providing access regime in the guarded sites and / or
- video surveillance and / or
- monitoring control, which is a limited form of video surveillance – technical monitoring of the protected site, without the ability to record the data

[2] "Electronic persons- new uses of legal personality", Dr. Stoyan Stavrov, collection of reports from a scientific conference of the Law Faculty of Sofia University, held on 15.05.2017[9].

obtained, but with the ability inform the movement of persons and objects, and

- undertaking actions in case of unlawful encroachment on the protected property and / or natural person in the site in accordance with § 1, item 6 of the Additional Provisions of the Private Security Business Act.

The protection of the property can also be performed by means of uses security alarm systems[3].

What is said in this part defines the scope of the specific tasks that can be set before the robotic system generally in the field of security activities. Additional consideration is also due regarding the environment in which the impact takes place-urbanized environment. The present study makes sense to explore the relations in urban areas from the point of view of the practical significance of the most common hypothesis for the environment in which security actions are performed, as well as from the point of view of the specific interaction of different technical requirements, including and public and private legal regimes in the context of the activity in question. With regard to the environment in respect of which the task is implemented, should be noted that urbanized territories are defined in special law[4].

In conclusion, the scheme of the usable robotic system in the context of its application according to the national regulation of the private security activity, should be defined as:

1. task – protection of property, protection of persons;
2. study of the environment through sensors – in the implementation of monitor control, video surveillance, motion sensors, smoke, change, etc.;
3. impact on the environment through actuators – action regarding signaling to a control point, actions regarding permission / blocking of access, actions for counteraction.

The environment to which it is applied is a specific object with the specificity that it is located in an urban environment, understood according to its legal definition in which the actions performed by the robotic system can be performed on the surface or air or water, which presupposes independent specifics.

All the described technical characteristics and technological specifics of the provision of private security services are classified and structured (see Figure 2), aiming to much those activities with the previously described high-level robotic system model.

---

[3] Defined in § 1, item 4 of the Additional Provisions of Private Security Business Act as alarm systems against intrusion and attack, involving central or local boards, control panels, sensors, alerting means and devices for transmission of signals over a distance that send alerts of attempt at overcoming or destructing physical barriers of physical protection systems or upon attack of an object.

[4] Art.7 of Law on Spatial Planning, promulgated, State Gazette No. 1/2.01.2001 [11], as nucleated settlements, dispersed settlements and industrial parks outside the areas of the nucleated settlements and the dispersed settlements.

3. The current legal regime

Following the above understanding, the study focuses on the current legal regulation of the activity and especially on three aspects:

- video surveillance activity,
- the activity of processing the data from the video surveillance and
- taking action in case of unlawful encroachment on the protected property.

For precision is noted that at this stage we do not consider the possibility of using robots to take direct action to protect / counteract the perpetrator in case of unlawful encroachment on the protected property or person, due to existing legal prohibitions and additional considerations at the level of European regulation, which are systematically discussed below. Thus, we focus our research on the use of robots in the field of monitoring the territory through sensors, and the impact on the environment through the appropriate transmission of data and their possible processing, as the simplest possible model. The proposed model can be used in further developments in the specific subject area.

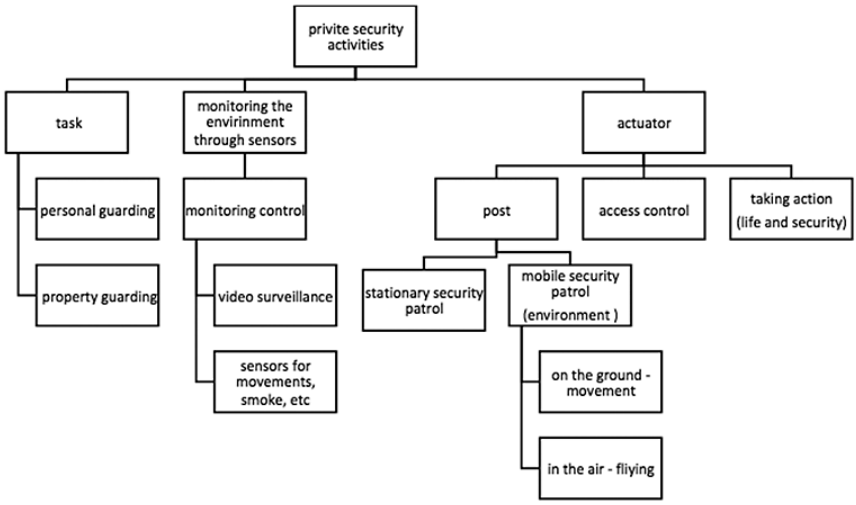

Figure 2: Private security activities classification

For precision is noted that at this stage we do not consider the possibility of using robots to take direct action to protect / counteract the perpetrator in case of unlawful encroachment on the protected property or person, due to existing legal prohibitions and additional considerations at the level of European regulation, which are systematically discussed below. Thus, we focus our research on the use of robots in the field of monitoring the territory through sensors, and the impact on the environment through the appropriate transmission of data and their pos-

sible processing, as the simplest possible model. The proposed model can be used in further developments in the specific subject area.

The activity of video surveillance according definition[5] is understood as the implementation of a technical form of processing and storage of personal data for the period provided by the law. This concept includes taking of photographs or filming of persons in a protected object and recording of the received data. Each activity should be in compliance with the provisions of the Personal Data Protection Act and its requirements for the processing of personal data.

Data capture inevitably raises questions about the legal context of captured images. The law is clear: The image of a person photographed on camera is a "personal data"[6].

Based on this understanding there is also a need to define the terms and concepts of processing and profiling provided in accordance with the existing regulations applicable in our national legislation and understood as:

- Processing of personal data is considered any operation or set of operations performed with personal data or a set of personal data, which is made by automatic or other means such as collection, recording, organization, and structuring, storing, adapting or modifying, retrieving, consulting, using, disclosing, transmitting, disseminating or otherwise making data available, arranging or combining, restricting, deleting or destroying[7].
- Profiling is any form of automated processing of personal data, expressed in the use of personal data to assess certain personal aspects related to an individual, and in particular to analyze or forecast aspects related to the performance of professional duties of that natural person, his economic condition, health, personal preferences, interests, reliability, behavior, location or movement[8].

That is important because in the considered hypothesis it is possible to use cameras for facial recognition, which allow remote biometric identification performed by a video surveillance system and may fall under the hypothesis of an automated solution. This, in turn, presupposes that recital 51 of the GDPR states that "when photographs or video recordings are processed by special technical means allowing unique identification or authentication of an individual, biometric

[5] § 1, item 3 of the Personal Data Protection Act, promulgated, SG No. 1/4.01.2002 [12].

[6] Within the meaning of Article 2 (a) of Directive 95/46 [13], in so far as it allows the person to be identified (decision of 11 December 2014). Ryne, C-212/13, item 22, CEC), adopted also in Decision № 13 of 14.09.2021 of the Bulgarian Supreme Court of Cassation on civil case file 96 4896/2019, IV year, Judge Zoya Atanasova. [14].

[7] According to art. 4, item 2 of Regulation 2016/679 of the European Parliament and of the Council of 27.04.2016 [15].

[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 [16] on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing of Regulation (EC) № 45/2001 [17] and Decision № 1247/2002/EC [18].

processing takes place". The GDPR prohibits the processing of special categories of personal data, including "biometric data", except in cases where any of the explicit exceptions under Art. 9 (2) of the Regulation. Biometric data[9] are "personal data obtained as a result of specific technical processing, which are related to the physical, physiological or behavioral characteristics of a natural person and which allow or confirm the unique identification of that natural person as facial images or dactyloscopic data. This is due to compliance with additional restrictions on the processing of biometric data for remote identification of public places such as biometric or facial recognition is implemented or used only by public authorities of Member States for purposes of essential public interest (Art. 12) [12].

In the general case, it is evident from the published analysis of the summary practice of the Bulgarian Commission for Personal Data Protection (CPDP) after May 25, 2018 on issues related to video surveillance, in the information bulletin of the CPDP for November-December, 2021 [12] that when video surveillance is carried out to assess its legality in the context of compliance with the provisions of Regulation (EU) 2016/679 should take into account [15]:

- the existence of a legitimate purpose of video surveillance;
- the legal basis for the processing of personal data by technical means of video surveillance[10];
- the right for information. The natural person subject to video surveillance to be notified of the use of technical means of surveillance in the site;
- the existence of appropriate technical and organizational measures for data security[11].

In the particular field of security activities, there is a purpose of video surveillance provided by a special law and a legal basis for processing personal data. Therefore, to meet the initial requirements and the criterion of lawfulness it is necessary to have a notice to person subject to video surveillance, made in an appropriate manner and relevant technical and organizational measures.

The observance of these conditions is also subject to the principle of proportionality as an element of the principle of the rule of law, established by the law[12], according to which the restriction of constitutionally protected rights must be proportionate to the legitimate aim pursued, and not to goes beyond what is necessary to achieve it. Therefore, in some cases additional considerations are needed to ensure legality, and it is necessary to assess the capture and processing of data by video surveillance in three aspects:

---

[9] Art. 4, item 14 of the General Regulation

[10] Under Art. 6, § 1 of Regulation (EU) 2016/679.

[11] Art. 24 of Regulation (EU) 2016/679

[12] Art. 4, para. 1 of the Constitution of Republic of Bulgaria (Decision № 14 of 2014 on COD № 12/2014; Decision № 2 of 2015 on COD № 8/2014; Decision № 7 of 2019 on Code № 7/2019; Decision № 11 of 2021 on Code. 7/2021) [19].

1. The recording of data related to the ordinary use of the property. Within a video surveillance data related to the personal life and household activities of the persons, owners or residents of the property – object of security and users of the video surveillance service can be recorded. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Art. 32 of the Constitution of the Republic of Bulgaria elevate the right to privacy and family life as a fundamental freedom [19]. Therefore, video surveillance systems should only be used for security purposes and for no other purpose. They cannot be used to monitor presence or behavior or to investigate various purposes, unless it is an incident related to physical security and safety or for a criminal act, where they are again used as evidence[13].

2. The recording of data in which, simultaneously with the observation of the site, data related to common parts, which are shared by other persons on legal grounds, are recorded but without these persons being users of the security service and without having given their consent, or on public sites. With regard to the implementation of video surveillance in condominium ownership, it is necessary to comply with a number of specific requirements arising from the special legal framework[14].The processing is based on art. 6, § 1, b "f" of Regulation (EU) 2016/679 and it is necessary to take into account the requirement of Art. 17, para. 3 of the Condominium Ownership Management Act, namely: the decision should be taken by the majority of more than 50 percent of the presented ideal parts of the common parts of the condominium. Based on court practice[15], it is now clear that the decision to conduct video surveillance is also mandatory for owners who have submitted a notification that they do not wish to be filmed. About video surveillance installed in the common parts of a residential building and court, agree it in order to pursue legitimate interests, such as ensuring the security and protection of persons and property. Without the consent of the persons concerned, if the processing of personal data by the video surveillance system in question meets the conditions set out in referred to in Article 7 (f) of the Charter of Fundamental Rights of the European Union.

---

[13] Under the sanction of the Criminal Procedure Code promulgated, State Gazette No. 86/28.10.2005.

[14] Condominium Ownership Management Act, promulgated, State Gazette No. 6/23.01.2009 [20].

[15] In this sense is the Judgment of the Court (Third Chamber) of the European Union of 11 December 2019, TK v. Asociaţia de Proprietari bloc M5A-ScaraA, Reference for a preliminary ruling Case C-708/18. [21], which states that Article 6 (1) (c) and Article 7 (f) of Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, in conjunction with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as allowing national provisions authorizing the introduction of a video surveillance system such as that at issue in the main proceedings Decision № 39 of 19.02.2013 on the case № 657/2012, G K., I G O. of the Supreme Court of Cassation.

Regarding the video shooting of public objects. The principle consistently advocated by the Bulgarian CPDP is that private entities are not allowed to photograph public places such as public areas serving an unlimited number of people, streets, metro stations, sidewalks, squares, parking lots and others. Typically, when video surveillance is used for security purposes to protect a legitimate interest (one's own or a third party's), data controllers must position the video cameras in such a way as to capture only the protected object. If this is not the case, the video surveillance /recording of public areas should be stopped by redirecting the camera or adjusting the angle of video recording so that it captures only the boundaries of the own / guarded property. If it is impossible to redirect the camera, if possible, a system for blurring in public places is introduced, or if this is not possible too, the video cameras that perform video surveillance in public places and foreign properties should be removed. Another case is when the video surveillance is carried out in the public interest for protection of public order and security by a public body, with duly provided information about it.

4. The recording of data related to illegal intrusion into the property – object of the provided security service

In its relatively newly established practice[16], the Supreme Court of Cassation confirmed, that it is incorrect to consider that accidentally created photographs, slides, film recordings, video recordings, etc., which reflect or contain information about circumstances included in the subject of proof, should be mixed with the relevant material evidence[17]. In the same decision, the Supreme Court of Cassation reaffirmed its practice that accidentally created photo, video, film recordings, etc. incl. recordings created by means of cameras placed in public areas may be used as evidence in view of their ability to contribute to the disclosure of the truth. In case of doubt, their authenticity can be verified by all procedural methods, incl. and by expert means[18]. However, insofar as no one can be monitored and recorded without his knowledge[19], it should be proved that the recording was not made secretly, i.e. is made with the knowledge of the subject (through information about the presence of species surveillance) or with the consent of the subject, which is obviously not likely in case of illegal behavior.[20]

---

[16] Decision № 206 of 15.01.2019 of the Supreme Court of Cassation under case file № 913/2018, III no., Judge Milena Paneva [22].

[17] Referred to in Art. 125, para. 1 Criminal Procedure Code.

[18] For example, R-390-2009 under case № 393/2009, SCC, II no.

[19] According to 32, para 2 of the Constitution of Republic of Bulgaria.

[20] In this sense, Decision № 456 of 14.11.2012 on k. n. d. № 1388/2012 SCC, I p. department [23].

Regarding secret surveillance, the case of the European Court of Human Rights (ECtHR), 10764/09, Cabrera v. Spain, is known[21], again raising the issue of the violation of this fundamental right – the right not to be enrolled without your knowledge. This practice should be complied with, but the special norm of the Bulgarian legislation should also be attached, namely that the executive act related to the production, use, sale or possession of a special technical device intended for covert/ secret collection of information without proper permission, which is required by law, is a crime[22]. However, on clandestine video surveillance, even for lawful purposes, restrictions are in place. The actions of even public authorities[23] must be clear and predictable; stating the scope of the assessment given to the authorities and the manner in which it was exercised with sufficient clarity; taking into account the legitimate aim of the measure in question; and to provide individuals with adequate protection against arbitrary interference.

In order to store video surveillance data, as part of their processing, it is also necessary to indicate certain specifics, such as the mandatory requirement in the Private Security Business Act for a specific retention period – 2 months, and the understanding that the retention of CCTV records after the expiration of this term can be considered as subsequent processing of personal data. The consequence is that in order to be compatible with the initial, subsequent processing should be taken the consent of the data subject[24]. Interesting is the ruling in the Judgment of the Court[25] that rules that the usage of a video surveillance system for video recording of persons stored on a long-term storage device, namely, which is installed by an individual in his family house to protect the property, health and life of the owners of the house. As the system also covers public places, does not constitute processing of personal data when performing entirely personal or domestic activities within the meaning of this provision.

---

[21] Namely, based on an assessment of the balance of interests, the ECtHR decided that in this case Cabrera's insurer, which hired a detective agency to detect insurance fraud committed by Cabrera, including through video surveillance and recording, acted in public interest, which prevails over the infringement of Cabrera's right. According to the ECtHR, it is a fact that interference in Cabrera's private life is present, but it is overcome because: the recording was made in a public place, made by a licensed detective company and the video is intended to serve as evidence in court.

[22] Within the meaning of Article 339a of the Penal Code.

[23] For example, the Savovi v. Bulgaria case, the ECtHR judgment of 27 November 2012 in the Savovi v. Bulgaria case, on appeal № 7222/2005, Fourth Section, President Ineta Ziemele [24], the European Court of Human Rights (Fourth Section), Amann v. Switzerland [GC]) , № 27798/95, § 56, ECHR 2000-II, and Liberty and Others v. The United Kingdom, № 58243/00, § 62, 1 July 2008.

[24] In view of Art. 6, § 4 of Regulation (EU) 2016/679.

[25] Judgment of the Court, Fourth Chamber of 11 December 2014, CEC, František Ryneš v Úřad pro ochranu osobních údajů. Reference for a preliminary ruling from the Nejvyšší správní soud. [25] which, although under the repealed Regulation, we consider to not have lost its legal significance.

In an attempt to systematize, the information is presented as a table (see Table 1), which consists of a list of these regulatory acts, as a general and specific legal framework for individual types of security activities.

Table 1

Legal regulations by security activity

Type of security activity	Legal regulation – general regime	Legal regulation – specific regime
Video surveillance activity	Private Security Business Act Personal Data Protection Act Directive 95/46 Regulation 2016/679 of the European Parliament and of the Council Regulation (EU) 2018/1725 of the European Parliament and of the Council Regulation (EC) № 45/2001 Convention for the Protection of Human Rights and Fundamental Freedoms Constitution of the Republic of Bulgaria Criminal Procedure Code Condominium Ownership Management Act	European Parliament resolution of 16 February 2017 (2015/2103 (INL), European Parliament resolution of 20 October 2020 (2020/2014 (INL), European Parliament resolution of 20 October 2020 (2020/2012 (INL)
Processing the data	Private Security Business Act Personal Data Protection Act Directive 95/46 Regulation 2016/679 of the European Parliament and of the Council Regulation (EU) 2018/1725 of the European Parliament and of the Council Regulation (EC) № 45/2001 Convention for the Protection of Human Rights and Fundamental Freedoms Constitution of the Republic of Bulgaria Criminal Procedure Code Condominium Ownership Management Act	European Parliament resolution of 16 February 2017 (2015/2103 (INL), European Parliament resolution of 20 October 2020 (2020/2014 (INL), European Parliament resolution of 20 October 2020 (2020/2012 (INL)
Taking action in case of unlawful encroachment	Private Security Business Act Convention for the Protection of Human Rights and Fundamental Freedoms Constitution of the Republic of Bulgaria Criminal Procedure Code	European Parliament resolution of 20 October 2020 (2020/2014 (INL), European Parliament resolution of 20 October 2020 (2020/2012 (INL)

5. Problems and challenges in the legal regulation of the use of service robots in security

The first part of the study attempted to define the regulations that set the legal frameworks with which CCTV operators, including those licensed under the special law should comply, whether or not they use service robots. In case they use such assistants, they should provide those technical specifications guaranteeing the legal requirements laid down as a basic element for legality.

Also, it is due prior consideration that the use of a robots in the implementation of security is carried out only in the part of video surveillance and monitor control, respectively. Robots are not supposed to be used in actions related to securing the observation post as a stationary security patrol ensuring a pass regime and/or taking action in case of unlawful encroachment on the protected property or in the presence of imminent danger to the protected person.

Accordingly, the existing legal regime of video surveillance is necessary to upgrade by the legal regulations that arises from the characteristics of the used technologies. By the meaning of that:

- The first problem is generated from the mobility of the used devices. In the absence of an explicit text in the law that allows the use of mobile devices questions arise:
  a) related to the data obtained from the filming of objects and persons other than the protected object – accidentally falling within the scope of the filming, including with regard to their biometric data;
  b) the legal consequences of capturing a specific fact, given the correct identification of its geographical location.

The logic to be followed in the resolution of this legal problem is already discussed in Bulgarian court practice[26], related to the use of mobile technical devises by the traffic police in the application of the Traffic Code. The decision prescribes that the designation of the place detected and recorded by a mobile technical devise only by using the GPS system and the adopted geographical designation of the location (north latitude and east longitude in degrees) is not sufficient to locate the place of the offence.

- The second legal issue relates to the characteristics of cyber-physical systems, autonomous systems, intelligent autonomous robots and their subcategories[27], is about ensuring safety and security in their use, as well as resolving the ethical issues that arise in their use, identified in the resolution,

[26] Interpretative Decision No. 1 of 26. 02. 2014 of the Supreme Administrative Court in case No. 1/2013, Judge Lozan Panov [26].

[27] As named in the European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework for the ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL) [3].

for which there is no uniform legal regulation. These are to ensure the application of the principles of acting in the best interests of users – not causing harm to users and third parties. And autonomy and fairness; respect and observance of fundamental rights (such as human dignity, equality, fairness and equity, non-discrimination, informed consent, protection of privacy and family life and data protection); avoiding stigmatization and applying the principles of transparency, autonomy, individual responsibility and social responsibility.

- The third legal problem is related to the lack of a clear solution on how to implement legal liability in the use of robots. In fact, it must be assumed that there is some clarity with the recommendations given in the European Parliament Resolution[28] in the specifically defined order of allocation of responsibility.

In this direction, the following risks are highlighted in the reflection on the legal regulation[29], namely the high risk of violation of fundamental freedoms related to privacy and data protection,

1. because the devices used are mobile and can position and transmit data from spaces that are traditionally secure and private, and
2. because there is a hypothetical possibility that applications and appliances that communicate with each other and with databases without human intervention can transmit and process, exchange and store data unlawfully, and
3. there is the separate and independent possibility of transmitting sensitive biometric data and profiling.

Reference should also be made to European Citizens' Initiative[30], relating to a request to ban mass biometric surveillance in the EU, profiling and forecasting is a threat to the rule of law and our most basic freedoms. The use of mass biometric surveillance in Member States and by EU agencies has led to violations of EU data protection law and has unduly restricted people's rights, including the right to privacy, the right to freedom of expression, the right to protest and the right to non-discrimination. In this sense, the predictability of legal regulations is also difficult to assess, as social relations evolve and change under the influence of various socio-economic factors.

---

[28] European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, (2020/2014(INL) [2].

[29] Also mentioned in the European Parliament Resolution of 16 February 2017 with recommendations to the Commission on civil law rules on robotics (2015/2103(INL) [1].

[30] Commission Implementing Decision (EU) 2021/27 of 7 January 2021 on the request for registration of a European Citizens' Initiative entitled "Civil Society Initiative to ban mass biometric surveillance practices' (notified under number C(2021) 32) [27] The citizens' initiative calls for an end to "automated recognition in public places of human characteristics, not only of faces, but also of gaits, fingerprints, DNA, voices, keystroke dynamics, and other biometric or behavioral signals."

6. Possible approaches and solutions

At this stage, legal regulation exists for some of the issues raised, and is actively being developed based on existing legal principles and mechanisms.

In terms of safety and security, the need for international harmonization of technical standards is recognized and adopted as an approach, in particular together with the European standardization organizations and the International Organization for Standardization committee on robotics ISO/TC299 dedicated exclusively to the development of standards in the field of robotics. Also introducing deliberate requirements with an appropriate legislative mechanism[31].

The need to introduce safeguards, guarantees and the possibility of human control and verification in automated and algorithm-based decision-making. In fact, in the European Union there is a prohibition expressly regulated by Art. 22 of the GDPR, which states that a person has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, an exception being allowed only where permitted by Union or Member State law. It would be true to say[32], that the European Union has chosen the main guiding element in legal regulation to be security. The last one is based on the view that, despite the characteristics of "autonomy" and "adaptability", one of the key requirements for the policy of regulation of artificial intelligence and robots is based on "human factor and supervision" and be a risk-based approach adopted.

Possible legislative regimes to registrar or licensing of cyber-physical systems, autonomous systems, intelligent autonomous robots and systems using artificial intelligence are derived. As well as the development of additional regimes the construction of a mandatory tracking and identification system[33] to allow the location of the aircraft in use to be determined in real time.

The introduction of technical requirements as legal principles to be traced and controlled at the design level[34]. These are, for example:

a) the reversibility principle, in which the reversibility model tells the robot which actions are reversible and how to undo them, with the ability to undo the last action or series of actions allowing;

---

[31] For example the European Parliament Resolution of 29 October 2015 on the safe use in civil aviation of remotely piloted aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs) (2014/2243(INI))) [28].

[32] As described in the analysis of the future European legislative framework for artificial intelligence and personal data protection in automated decision-making, made by Prof. Dr. Irina Tsakova [29].

[33] For example, with regard to the use of unmanned aerial vehicles, understood remote-controlled, automated, connected and autonomous aircraft the measures referred to in Regulation (EC) № 216/2008 of the European Parliament and of the Council.

[34] As an example in this regard, described in the European Parliament Resolution of 16 February 2017, containing recommendations to the Commission on civil law for robotics (2015/ 2103 (INL) [1].

b) the requirement that these automated systems be equipped with a "black box" that records the data for each operation performed by the machine, including the logical operations that helped to make its decisions, etc.

The use of known approaches in solving this type of hypothesis. For example, the approach, which regulates the use of RFID technology and allows the transmission of short distances of data, including personal data, without physical contact or visible interaction between the reader or writer and the label, so that the interaction can take place without the individual concerned[35]. The data encryption approach[36] allows personal data to be encrypted in electronic format during storage or transfer, with keys managed and stored separately, appropriate standard algorithms used and appropriate keys should be used in accordance with international standards (such as the ETSI standard) and provides the ability to manage keys, and all keys and passwords are protected against unauthorized access. As well as the known and existing regulations for guarantee funds and insurances, regulations related to the collective exercise of rights and liability, etc.

Use of the model set out in the European Parliament Resolution of 20 October 2020 with recommendations to the Commission on the regime of civil liability for artificial intelligence (2020/2014 (INL) [2] on the allocation of legal liability.

7. Conclusion

The legal regulation of the use of service robots in the implementation of security activities in urban environments should define the function and scope of the activities of service robots and their safety through technical standards and certification. As well as a legal mechanism to ensure that in the performance of their functions they will process and exchange personal data in the scope and manner defined by law, and, accordingly, it will not be possible to reach a decision based solely on automated data processing.

For now, the legal liability in case of damaging actions of the used robots, assuming that they fall within the definition of autonomous systems using artificial intelligence, should be undertaken by the operator of the system alone, or by the operator of the system and the affected person, if he/she has caused the damage by his/her actions, as well as possibly in a joint liability regime – by two or more operators, subject to the possibility of recourse in case of applicability. In the event that the robots are not defined as an autonomous system with artifi-

[35] Adopted in 2009/387 / EC: Commission Recommendation of 12 May 2009 on privacy and data protection in applications using radio frequency identification [30].

[36] Described in Commission Implementing Regulation (EU) 2019/1799 of 22 October 2019 laying down technical specifications for individual online support collection systems under Regulation (EU) 2019/788 of the European Parliament and of the Council on the European Citizens' Initiative [31].

cial intelligence in view of its characteristics, then the rules of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for damage caused by a defect in a product (OJ 1985 L 210, 7. 8. 1985, pp. 29), respectively the transposed national text.

A high level model for the task, the sensor part and the actuators used in the provision of security activities in an urban environment by service robots was proposed. The proposed model could be used when considering the regulatory framework governing the activity in question.

8. Acknowledgements

This paper is prepared with the support of MIRACle: Mechatronics, Innovation, Robotics, Automation, Clean technologies – Establishment and development of a Center for Competence in Mechatronics and Clean Technologies – Laboratory Intelligent Urban Environment, funded by the Operational Program Science and Education for smart growth 2014-2020, Project BG 05M2OP001-1.002-0011.

9. References

[1] European Parliament resolution of 16 February 2017 with recommendations to the Commission on civil law on robotics (2015/2103 (INL)).

[2] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a regime of civil liability for artificial intelligence (2020/2014 (INL)).

[3] European Parliament resolution of 20 October 2020 with recommendations to the Commission on framework for the ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).

[4] M. Nisheva, D. Shishkov, Artificial Intelligence, ISBN: 954-8643-11, Integral, 1995, Bulgaria.

[5] Vasil Georgiev, Ioannis Patias, Hristo Hristov, Autonomous Systems: Platforms, Applications, Perspectives – ISBN: 978-954-07-5033-0, University Publishing House "St. Kliment Ohridski", Bulgaria, 2020.

[6] Ioannis Patias, Vasil Georgiev, Design of Robotic Systems, ISBN: 978-954-07-4207-6, University Publishing House "St. Kl. Ohridski", 2017.

[7] Sostero, M., Automation and Robots in Services: Review of Data and Taxonomys, Seville: European Commission, 2020, JRC1218933.

[8] "Electronic persons- the new uses of legal personality", Dr. Stoyan Stavrou, collection of reports from a scientific conference of the Law Faculty of Sofia University, held on 15.05.2017.

[9] Decision № 13 of 14.09.2021 of the Supreme Court of Cassation on the case № 4896/2019, IV d., Judge Zoya Atanasova.
[10] Private Security Business Act, Promulgated, SG No. 10/30.01.2018.
[11] Law on Spatial Planning, promulgated, State Gazette No. 1/2.01.2001.
[12] Personal Data Protection Act, promulgated, SG No. 1/4.01.2002.
[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, https://app.eurocases.eu.
[14] Analysis of the summarized practice of the Commission for Personal Data Protection /CPDP/ after May 25, 2018 on issues, related to video surveillance, in the information bulletin of the CPDP for November-December, 2021.
[15] Regulation 2016/679 of the European Parliament and of the Council of 27.04.2016 https://app.eurocases.eu.
[16] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 https://app.eurocases.eu.
[17] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, https://app.eurocases.eu.
[18] Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties, https://app.eurocases.eu.
[19] Constitution of Republic of Bulgaria.
[20] Condominium Ownership Management Act, promulgated, State Gazette No. 6/23.01.2009.
[21] Judgment of the Court (Third Chamber) of the European Union of 11 December 2019. TK v Asociaţia de Proprietari bloc M5A-ScaraA. Reference for a preliminary ruling from the Tribunalul Bucureşti, Case C-708/18.
[22] Decision № 206 of 15.01.2019 of the Supreme Court of Cassation under case № 913/2018, III no., Penal dep., Judge Milena Paneva.
[23] Decision № 456 of 14.11.2012 on case № 1388/2012 SCC, I penal dep.
[24] Judgment of 27 November 2012 of the ECtHR in the case of Savovi v. Bulgaria, on appeal № 7222/2005, Fourth Section, European Court of Human Rights (Fourth Section) President Ineta Ziemele.
[25] Judgment of the Court (Fourth Chamber) of 11 December 2014. František Ryneš v Úřad pro ochranu osobních údajů. Reference for a preliminary ruling from the Nejvyšší správní soud.
[26] Interpretative decision № 1 of 26.02.2014 of the Supreme Administrative

Court case № 1/2013, Judge Lozan Panov.
[27] Commission Implementing Decision (EU) 2021/27 of 7 January 2021 on the application for registration of the European Citizens' Initiative entitled "Civil Society Initiative Banning Mass Biometric Surveillance Practices" (notified under document C (2021) 32).
[28] European Parliament resolution of 29 October 2015 on the safe use in civil aviation of remote-controlled aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs (2014/2243 (INI))).
[29] The future European legislative framework of artificial intelligence and personal data protection in automated decision-making, Prof. Dr. Irina Tsakova.
[30] Commission Recommendation of 12 May 2009 on compliance with the principles of privacy and data protection in applications using radio frequency identification.
[31] Commission Implementing Regulation (EU) 2019/1799 of 22 October 2019 laying down technical specifications for individual online support collection systems pursuant to Regulation (EU) 2019/788 of the European Parliament and of the Council on European Citizenship initiative.