Domazet Siniša[*]
https://orcid.org/0000-0002-5964-2249
Marković M. Darko[**]
https://orcid.org/0000-0001-9124-6417
Skakavac Tatjana[***]
https://orcid.org/0000-0002-5017-176X

UDC: 342.7:004.378.5
Review article
DOI: 10.5937/ptp2403109D
Received on: July 18, 2024
Approved for publication on:
September 14, 2024
Pages: 109–124

PRIVACY UNDER THREAT – THE INTERSECTION OF IOT AND MASS SURVEILLANCE

ABSTRACT: The rapid development of information and communication technologies, blockchain technologies, artificial intelligence (AI), as well as the Internet of Things (IoT) devices has brought numerous advantages to modern society. Alongside increased comfort of life and efficiency in all areas of human activity, the automation enabled by interconnected networks also poses a challenge to citizens' right to privacy. The goal of this research is to identify weaknesses in this use of modern technologies, specifically in how they negatively impact the citizens' right to privacy, by analyzing the relationship between mass surveillance practices and IoT devices. The research established that the implementation of mass surveillance measures using IoT technology can lead to violations of ethical standards, security protocols, and the right to privacy. It has been shown that there are issues with applying existing regulations to IoT and mass surveillance and that no universal legal framework currently exists to protect the right to privacy. The use of IoT technology, especially given the rapid development of artificial intelligence, will in the future

[*]LLD, Full professor, Metropolitan University, Belgrade, Serbia, e-mail: sdomazetns@gmail.com
[**]LLD, Associate professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: darko.markovic@pravni-fakultet.edu.rs
[***]LLD, Associate professor, Union University, Belgrade, Faculty of Law and Business Studies dr Lazar Vrkatić, Novi Sad, Serbia, e-mail: tatjana.skakavac@gmail.com

raise numerous dilemmas regarding the entities responsible for collecting personal data, the consents required for data usage and processing, where the collected personal data will be used, and for what purposes. Therefore, it is necessary to adapt privacy laws to modern technological advancements such as IoT and AI. This study utilized methods of induction, deduction, and content analysis.

Keywords: *Internet of Things, artificial intelligence, privacy, security, personal data collection.*

1. Introduction

The rapid development of information and communication technologies, blockchain technologies, artificial intelligence, as well as the Internet of Things (Internet of Intelligent Devices) has led to numerous advantages for modern society. However, in addition to its potential to improve efficiency, convenience, and quality of life, the growing use of IoT raises concerns about privacy rights and security overall, especially in the context of interacting with mass surveillance. The Internet of Things has become not only an expression of networked computing based on cameras, databases, smart sensors, softwares, but also a means of mass surveillance during which data is collected and exchanged. This becomes a problem when personal data is collected, including biometric data and information about personal habits and preferences, as well as location.

The existence of a mass global surveillance system was revealed to the world public by former US government official Edward Snowden at the Web Summit in Lisbon's Altice Arena in 2013. The knowledge that the system of collecting personal data of citizens was built through the surveillance of smart devices that people use, and for which they use the Internet (mobile phones, laptops, computers and any other device that can be connected to the Internet), shocked the world. The discovery that the violation of personality is practically legalized through the violation of privacy has forced the question of the ethics of mass surveillance and the limits of the justification of security reasons for violating the privacy of citizens. The indisputable fact, which is not even denied, that the possibilities of mass surveillance are progressively growing thanks to the Internet of Things and artificial intelligence, caused an increase in the interest of not only the scientific and professional public in this phenomenon, but has also forced states and international organizations to deal more seriously with this phenomenon.

Bearing in mind the above, by combining the methods of content analysis, induction and deduction, the paper analyzes the interaction of the Internet of Things and mass surveillance, with the aim of identifying weaknesses in this use of these technologies, which negatively reflect on citizens' right to privacy.

2. IoT and mass surveillance: A complex web of data, devices, and ethics

Modern times are increasingly characterized by the influence of new technologies in the everyday life of citizens, which further complicates security issues. Modern technologies have also created the need to develop the security of information systems (Marković & Dostić, 2019, p. 173). Networking of information systems, as well as individual devices, leads to a significant increase in their functionality. For this purpose, the IT sector strives to develop non-standard digitized devices intended for data exchange via the Internet, i.e. sending data and/or receiving instructions. Such devices are called intelligent, so this phenomenon was named the Internet of (intelligent) things (IoT), where it does not refer to a single device but to a network of devices and different objects (including buildings) that, being networked, collect and exchange data. In order to collect data, these devices and objects must be equipped with sensors, software and, in general, technologies that enable connection and exchange of data with other devices and systems. Based on the analysis of data collected through IoT devices, their users (business entities, organizations, governments...) can gain insight into trends and accordingly optimize work processes and improve the efficiency of decisions made (Zirojević & Ivanović, 2021, p. 202). These devices generate massive amounts of data, which can then be analyzed using machine learning and other data analysis techniques.

IoT will completely become a part of our homes, service activities, electricity supply, will be present in the production of various types of goods, and we should not ignore the area of security and the possibility of surveillance of citizens by governments around the world. At the same time, this development of IoT possibilities also indicates the growing potential of mass surveillance, no longer in public places (streets, shopping centers, stadiums and other objects and spaces of free movement and assembly) but also in objects and spaces that are considered private.

Bearing in mind the usability of the Internet of Things in practice, in the period ahead, their applicability will grow, but also the possibility of misuse

in sensitive areas of social life. This especially applies to mass surveillance, which in itself is a source of potential threat to citizens' privacy, and the implementation of the Internet of Things makes this ethical and security-legal problem more complex.

From the very term mass surveillance, one can guess that it is about the simultaneous surveillance of a large number of people, with the engagement of a large number of operatives and/or a large number of technical devices. Bearing in mind the growing network of technical devices that are connected to the Internet and can collect and exchange data, in the context of the topic of the paper we speak of mass surveillance as "the indiscriminate monitoring of a population or a significant component of a group of persons" (Privacy International, 2020). However, it can also be organized for the purpose of "spying on the entire population or a significant part of it", which is carried out by states and corporations, by applying various methods based on physical activities and the use of various technical means, they collect not only information about the content of the activity being monitored, but also about all other , at first glance less significant data, which can sometimes play a crucial role in forming the necessary conclusions (Gammeltoft-Hansen & Vedsted-Hansen, 2017).

Due to the invasion of privacy, human rights and freedoms, mass surveillance is itself a cause of ethical concern. The intensity of this concern increases with the increase in the potential of mass surveillance, which is virtually limitless thanks to the availability of Internet of Things resources, and especially with the development of artificial intelligence. The practice of (mass) surveillance is adapted to the circumstances of application and the goals to be achieved, and most often includes methods and actions, such as

> *interception, collection, transmission of data from e-mails, eavesdropping on telephone conversations, 'intrusions' into computers, monitoring and data collection via social networks, but also the collection of so-called meta data (for example, about the time and place of sending a message or phone call)* (Domazet & Dinić, 2022).

In this regard, the case of the Chinese social credit system is particularly interesting, which according to some authors represents "one of the evolutionary forms of mass surveillance" (Domazet, Lubura, Šušak-Lozanovska & Ilik, 2021). Such widespread use of IoT in the function of mass surveillance simply neutralizes the possibility of control of sensitive personal data by citizens and

increases the risk of unauthorized access and surveillance, as well as misuse of data. In such circumstances, a number of ethical questions about consent, transparency and responsibility are further opened. This makes the problem more complex not only ethically, but also from a security and legal point of view. When it comes to solving ethical problems, organizations that use IoT for the purpose of mass surveillance should adopt ethical frameworks and guidelines, to ensure that the use of these devices is transparent and responsible, which also implies respect for the right to privacy of citizens.

3. Security implications of IoT in mass surveillance systems

Even when the use of IoT for the purpose of mass surveillance is within the limits of ethics, the security implications of such use cannot be ignored, and especially not when the principles of ethics are violated. The use of IoT for mass surveillance provides the potential for invasive data collection, which can then be used for political manipulation, marketing and other purposes, raising privacy and security concerns. In security circles, it is pointed out that practically every physical object in the very near future, thanks to the unique identification when connecting via the Internet (IP address), will create a kind of identity of an intelligent thing. Such a facility will be able to create a database of all activities on it, by type of activity, actors and event time, from the moment it leaves the production line. The final point in time cannot be known in advance, because the "intelligence" of such things will reach the ability to provide information on how to repair them, and in the event of a fatal end or damage, they will be able to give us instructions on recycling. Mutual communication and access will take place between such facilities "to the massive processing and storage capacities of the cloud, further strengthened by additional mobile and social networks" (Goodman, 2016).

These devices can be stolen or hijacked or, more commonly, hacked to gain unauthorized access to sensitive data and use the device for malicious purposes. To solve these challenges, it is necessary to implement a combination of security measures, such as encryption, authentication and access control, and thus protect the privacy and security of IoT data. Today, many technical devices, in daily personal use, have built-in chips with developed software for registration and recognition of biometric data (controlling a mobile phone, television, lighting, etc.). At the same time, biometric data does not mean only fingerprints or palm prints and DNA, but now also facial features, the shape of the ears, the characteristics of the irises, the way of walking, the characteristics of the voice, and even the way of breathing. With the help of software with

integrated artificial intelligence, security services around the world can more easily identify rioters at sporting events, perpetrators of criminal acts and, most importantly, terrorists. However, not only the potentials of application to protect the safety of citizens are growing, but also the potentials of arbitrary mass surveillance, i.e. misuse of IoT.

The privacy of individuals becomes virtually unprotected from the indiscriminate collection of data without their consent. It is possible to misuse the data collected in this way for political or other purposes, and in this regard, sensitive social groups (based on religious and/or ethnic affiliation or personal characteristics) are endangered, as well as those individuals and social groups whose political beliefs are unacceptable for the ruling elite. Investigative journalism can also be classified into this category, whose activities are hindered by the very knowledge of possible exposure to secret, even undisguised, surveillance, not only in public places but also in an environment that until recently was considered private, even intimate. For the same reasons, developing the feeling that they are under constant surveillance, restrains people's activities, restricts them to behavior that is not in the least contrary to the ruling policy, despite the awareness of its harmfulness. Here we are talking about the effect of latent intimidation that tends to spread to the entire society, and the goal is to create total power that is achieved "with complete politicization of all segments of social and individual life" (Marković, 2019, p. 11). In such circumstances, distrust develops among people – in each other, as well as in institutions. As a consequence, a culture of snitching develops, characteristic of totalitarian societies, such as Nazism, fascism or Stalinism, as still fresh historical examples.

4. The legal dimension of IoT in mass surveillance: Challenges and solutions

The extremely fast development of modern technologies does not keep up with the legal regulations, especially in the part related to the protection of privacy and personal data of citizens. It can be said that in these areas the situation is becoming worrisome, given the lack of relevant legislation at the international level. Gradual progress can be seen from 2021, when "some countries have started to introduce certain mandatory security requirements for certain categories of IoT devices, such as the United Kingdom" (Page, 2021). Some countries have defined guidelines, best practices, certificates or labeling efforts. Although some US states have implemented privacy protection provisions into local law regarding mass surveillance, problems

arise in jurisdictions in other states where such regulations are not applicable to a particular type of (Abendroth, 2022). According to the report on the use of IoT technologies, conducted by the US Government Accountability Office (GAO), 56 of the 90 federal agencies that responded to the GAO survey reported using Internet of Things (IoT) technologies, most often for: "(1) control or monitor equipment or systems (42 of 56); (2) control access to devices or facilities (39 of 56); or (3) track physical assets (28 of 56) such as fleet vehicles or agency property" (Page, 2021).

Most of these agencies indicated the expansion of the scope of IoT use and, in this regard, the increase in data collection activities and operational efficiency, which should contribute to easier decision-making and increased efficiency, i.e. enabling "agencies to accomplish more with existing resources" (GAO, 2020). From a privacy rights perspective, a 2016 statement by a former US director of national intelligence that "in the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" (Ackerman & Thielman, 2016) raises concerns. This is a very clear indicator of the ability of governments around the world to make the Internet of Things their tool for collecting various data about citizens.

There is no doubt that governments around the world, namely their national security agencies, have the right to collect data and information using the Internet of Things, given the possibility that individuals may use the Internet of Things to commit certain crimes or acts of terrorism. However, the problem arises in cases where governments use IoT capabilities in an illicit manner. The legal basis for combating such abuses in the US is defined by the Warehouse Records Act, 18 U.S.C. §§ 2701 et seq. This law restricts the right of state bodies to access the contents of wire and electronic communications, which is conditioned by the prior obtaining of a court order in the procedures established by the Federal Rules of Criminal Procedure, or "in the case of a State court, issued using State warrant procedures and, in the case of a court-martial […] in accordance with regulations prescribed by the President)" (United States Code, 1988). Regardless of the principle of "reasonable expectation of privacy", US jurisprudence has taken the position that "a computer user may have a legitimate expectation of privacy in the content of email communications"[1], "but where a person chooses to transmit that information to a third party, a person's 'reasonable' expectation of privacy

[1] *U.S. v. Lifshitz*, 369 F.3d 173, 363 F.3d 158 (2d Cir. 2004). Downloaded 2024, May 12 from https://caselaw.findlaw.com/court/us-2nd-circuit/1122505.html

may come to an end"[2]. Thus, in the US, the position is taken that if citizens voluntarily hand over personal data to third parties (for example, IoT device manufacturers) using IoT devices, then there is no reasonable expectation of privacy, and state authorities can collect data, i.e. carry out surveillance, without a court order.

During the COVID-19 pandemic, most countries introduced the application of mass surveillance into legal channels with the aim of ensuring the implementation of the ordered measures for the general safety of citizens (Matijašević & Ditrih, 2021, p. 25). In some of them (Poland, Singapore, South Korea, Russia) the Internet of Things was used in the form of GPS -enabled applications for tracking and restricting people's movements. In Hong Kong, movement control was begining at the airport itself, where arriving passengers were given special wristbands with a unique QR code for tracking. They were required to install the 'Stay Home Safe' app on their smartphones and scan the QR code from the wristband, which allowed the Hong Kong authorities to track their activities (Barker, 2020). There have also been accusations in the media that Russia is using Nokia's SORM equipment and software that allow the authorities to "digital surveillance to the nation's largest telecommunications network" (Satariano, Mozur & Krolik, 2022).

In the European Union, there is a discussion about legal solutions for the use of artificial intelligence, and the biggest stumbling block is precisely the possibility of misuse of biometric data (Mladenov, 2023, p. 36). Ella Jakubowska, a policy advisor in the European Digital Rights network, which is headquartered in Brussels, points out that the importance of the legal solutions discussed go beyond the borders of the European Union, because what the EU makes legitimate, countries in other regions of the world will also accept it as legitimate, which can be abused in countries with authoritarian regimes (Shaer, 2023). The privacy protection during mass surveillance is regulated by the General Data Protection Regulation (GDPR). However, Edward Snowden warned that the GDPR is not strong enough to solve the problem of tech giants violating people's privacy. He believes that the GDPR was initially poorly regulated, because "the problem isn't data protection; the problem is data collection", that is, in other words, spying on citizens is not a problem as long as it does not cause harm to other people, that is, as long as the collected data is kept so that it does not fall into the hands of anyone else (Verdict-Encrypt, n.d.). Regarding the monitoring of electronic communications of citizens on

[2] *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577 (1979). Downloaded 2024, May 3 from https://supreme.justia.com/cases/federal/us/442/735/

the territory of the European Union, in May 2023 the European Parliament adopted the Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, expressing concern

> *over EO 14086's failure to provide sufficient safeguards in the case of bulk data collection, namely the lack of independent prior authorisation, lack of clear and strict data retention rules, 'temporary' bulk collection, and lack of stricter safeguards concerning dissemination of data collected in bulk; points particularly to the specific concern that without further restrictions on dissemination to US authorities, law enforcement authorities would be able to access data they would otherwise have been prohibited from accessing* (European Parliament, 2023).

Even before the Internet of Things was brought into connection with mass surveillance, the questions of legal regulation of the functioning of the Internet were raised and are still open. The issue of privacy is particularly sensitive on social networks (Skakavac, 2020, p. 76), which are also becoming fertile ground for mass surveillance through the Internet of Things. Social media users are very often careless about protecting their personal data, including their personal photos, which often ends up in the wrong hands exposing them to risks of misuse (Domazet & Skakavac, 2018, p. 117). Lau (2019) warns about the mass surveillance of social networks, pointing to the activities of federal government agencies "as the Department of Homeland Security (DHS)" expanding their activities to collect information from social networks of a different nature, "including political and religious views, data about physical and mental health, and the identity of family and friends". The 'target' of such surveillance is not only US citizens, but also foreign citizens who express their intention to come to the USA. The monitoring of their communication and activities, and the collection of various private data about them, does not pose a problem for the American National Security Agency (NSA), because access to this information on its servers and without the knowledge of the court or Congress is enabled by "Microsoft, Yahoo, Google, Facebook, Apple, Youtube, Skype, AOL and PalTalk" (Adetunji, 2013).

Even more worrying are the statements of NSA Deputy Director Richard Ledgett in 2016 that "his agency is researching opportunities to collect foreign intelligence from biomedical devices and other internet of things (IoT) devices" (Abel, 2016), thus revealing that even pacemakers and other

biomedical equipment can be used to collect personal data and monitor the population.

The misuse of IoT has also already been noted in the education system. Thus, in the Chinese province of Guizhou, chips are installed in school uniforms, which enable the monitoring of students' movements, and the stated purpose of such monitoring is to alert them if the students leave the school premises at the time when they should be in class, or if they sleep during the class. This is combined with facial recognition technology, and there are no guarantees that this surveillance system is not being misused to monitor student activity outside of class (Newman, 2019). In Beijing, facial recognition technology through IoT is being implemented in practically all spheres of life. Thus, during the construction of new residential buildings, the so-called smart locks, with the aim of increasing the security of tenants through face detection, by controlling the entry of foreigners, but also for the purpose of suppressing illegal subtenancy. This measure goes so far as to "asks management to check on senior residents if they haven't entered or left their homes after a certain period of time" (Fingas, 2018).

Having decided to apply for membership in the European Union, Serbia also accepted the path of harmonizing its legislation with that in force in the EU. Thus, when the General Data Protection Regulation (GDPR) was adopted in the EU in 2018, Serbia adopted its Law on the Protection of Personal Data, with which it tried to get closer to the standards set in the EU. There are differences in the appointment and responsibilities of supervisory institutions, which is logical considering that the EU is not a state in the classical sense, but a community of states. Deviations that have greater significance and consequences result in milder punitive measures in the Serbian law than in the GDPR, which does not correspond to the state of security awareness in Serbia.

Therefore, it can be seen that misuse of IoT can occur in several forms, and therefore it is necessary to constantly work on improving the existing legal regulations and develop more effective ways of protecting citizens' personal data. Cases of violation of privacy by private companies are a particular problem, given that numerous cases of such behavior have been recorded so far, and the cooperation of states with private companies in order to implement mass surveillance (such as the case of the Chinese company Huawei). All of this shows that IoT problems will only escalate, and international cooperation is needed to prevent privacy breaches.

5. Conclusion

The variety of definitions and the lack of a universal definition of IoT indicate that it is a complex technology. Despite its many benefits, IoT brings with it many dangers for users. First of all, there is an increasingly noticeable trend in which the population fears the theft of personal data through IoT devices, and the danger of hacking is no less. Then, a growing number of companies around the world are planning to implement IoT devices in their own business, and many companies are already doing so. Therefore, it is necessary to additionally secure against the possibility of hacker attacks, and companies must develop and implement appropriate security standards in the protection of IoT devices. A particular problem is the possibility of IoT devices being used for population surveillance by governments and their agencies around the world. Understandably, the measures of monitoring the behavior of Internet users, i.e. the interception of their electronic communications, will not be disputed in cases where the interests of national security are threatened, or when the prevention of criminal acts, especially terrorist acts, is involved. However, the problem arises when the IoT is misused and indiscriminate mass surveillance of the population is carried out, leading to a massive invasion of privacy.

In practice, a large number of cases of abuse during the implementation of surveillance measures have been recorded, especially after the revelations of Edward Snowden, and this trend has the prospect of growth. Thanks to the development of artificial intelligence, in the future, an increasing number of IoT devices will be interconnected, which will allow governments around the world to use IoT technology to collect even the most intimate data about the individuals they are interested in. This indicates potential violations of ethical norms, security standards and the rights and freedoms of citizens. In the absence of universal legislation protecting the right to privacy, there are problems with the application of existing regulations to the Internet of Things and mass surveillance.

With the above in mind, the role importance of regulation makers at the national and international level regarding the Internet of Things will increase in the future. In this regard, the right to privacy is relatively well defined around the world, although there are different legal solutions in some countries the right to privacy is a constitutional category (Serbia), somewhere it is regulated by laws (too) (EU countries, Serbia…), while in some countries the right to privacy is not an autonomous right (China). If we look at the right to privacy in relation to IoT, it can be concluded that there is a lot of room for improvement. In terms of privacy and personal data protection, there is

a veritable patchwork of different regulations in the US, given that there are no universal regulations established at the federal level. Due to its nature, IoT technology knows no national borders, so the diversity of regulations in the bordering states of the federation facilitates opportunities for abuse. The legal framework for protecting the privacy of EU citizens is the GDPR, which is very thorough and restrictive. However, it turned out that there are weaknesses in the implementation during the activities of the US intelligence services on the territory of the EU, which is why the European Parliament reacted by adopting a resolution in May 2023, which requires finding a solution that would give GDPR priority in such situations as well, i.e. so that citizens EU had equivalent protection before American courts. In this regard, the forthcoming legal regulation of the use of artificial intelligence and, in particular, biometric surveillance will be of key importance for EU citizens. No less significant is the definition of standards for the use of IoT in private companies, both in terms of protection against cyber attacks, and in terms of the use of corporate IoT devices by governments and their security agencies.

Taking into account that the level of awareness of the right to privacy and the level of security culture as a whole are at an unsatisfactory level among the citizens of Serbia, a weaker penal policy reduces the effectiveness of its legal solutions in this area. In this regard, and not only because of this, in order to raise privacy standards to a higher level in Serbia, it is necessary to raise the training and education of employees in companies, public administration and other organizations whose operations encroach on the field of privacy, as well as citizens as individuals, to the level of strategy.

Considering the revelations given to the world by Edward Snowden, as well as numerous allegations of investigative journalism about the abuse of technologies for the purpose of mass surveillance, additional efforts must be made in the coming period, especially in the field of legal protection of privacy in the conditions of the development of artificial intelligence and IoT, and in in connection with that, increasingly sophisticated (covert) mass surveillance of the population. The right to privacy will have to be improved in a way that will ensure adequate protection of personal data in accordance with the potential of modern technologies, such as IoT. This will undoubtedly change the very concept of privacy, which will no longer be viewed in the same scope as before, especially if the users themselves decide to share personal data with third parties through IoT devices. Finally, it is necessary to further develop existing regulations related to the monitoring of electronic communications, given the relatively numerous cases of privacy abuse by governments and their security agencies that have been confirmed in judicial institutions.

Domazet Siniša
Univerzitet Metropolitan, Beograd, Srbija

Marković M. Darko
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Skakavac Tatjana
Univerzitet Union, Beograd, Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad, Srbija

PRIVATNOST POD PRETNJOM – UKRŠTANJE INTERNETA STVARI I MASOVNOG NADZORA

APSTRAKT: Brzi razvoj informaciono-komunikacionih tehnologija, blokčejn tehnologija, veštačke inteligencije, kao i interneta inteligentnih uređaja doveo je do brojnih prednosti za savremeno društvo. Uporedo sa povećanjem udobnosti života i efikasnosti u svim segmentima ljudskog delovanja, automatizacija koja se postiže putem međusobno povezane mreže istovremeno predstavlja i izazov za pravo građana na privatnost. Cilj istraživanja u radu je da se kroz analizu odnosa prakse masovnog nadzora i IoT uređaja, identifikuju slabosti koje se pri ovakvoj upotrebi savremenih tehnologija negativno reflektuju na pravo građana na privatnost. Istraživanjem je utvrđeno da u praksi sprovođenja mera masovnog nadzora korišćenjem IoT tehnologije može doći do kršenja etičkih normi, bezbednosnih protokola i prava na privatnost. Pokazalo se da postoje problemi u vezi sa primenom postojećih propisa na Internet stvari i masovni nadzor, kao i da ne postoji univerzalna zakonska regulativa koja bi štitila pravo na privatnost. Primena IoT tehnologije, posebno imajući u vidu brz razvoj veštačke inteligencije, u budućnosti će doneti brojne dileme u vezi sa subjektima koji prikupljaju podatke o ličnosti, saglasnostima za korišćenje i obradu ličnih podataka, gde će se tako prikupljeni lični podaci koristiti i u koje svrhe. Stoga je neophodno zakonsku regulativu prava na privatnost prilagoditi savremenim tehnološkim dostignućima, kao

što su IoT i veštačka inteligencija. U radu su korišćene metode indukcije, dedukcije i analize sadržaja.

Ključne reči: *Internet stvari, veštačka inteligencija, pravo na privatnost, bezbednost, prikupljanje ličnih podataka.*

References

1. Abel, R. (2016). *NSA may dabble in IoT surveillance*. Downloaded 2024, April 15 from https://www.scmagazine.com/brief/architecture/nsa-may-dabble-in-iot-surveillance
2. Abendroth, B. (2022). *How will government actions on IoT security impact the decisions I make today?* Downloaded 2024, May 12 from https://techcommunity.microsoft.com/t5/internet-of-things-blog/how-will-government-actions-on-iot-security-impact-the-decisions/ba-p/3295773
3. Ackerman, S., & Thielman, S. (2016). *US intelligence chief: We might use the internet of things to spy on you.* Downloaded 2024, April 15 from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper
4. Adetunji, J. (2013). *Gathering private information online is abuse of state power.* Downloaded 2024, April 20 from https://theconversation.com/gathering-private-information-online-is-abuse-of-state-power-15044
5. Barker, R. (2020). *Covid-19 creates numerous use cases for the Internet of Things, but are they legal?* Dawnloaded 2024, May 2 from https://www.withersworldwide.com/en-gb/insight/covid-19-creates-numerous-use-cases-for-the-internet-of-things-but-are-they-legal
6. Domazet, S., & Dinić, S. (2022). International legal aspects of mass surveillance and implications on privacy. *Kultura polisa, 19*(1), pp. 79–97, 2022, DOI: 10.51738/Kpolisa2022.19.1r.5dd
7. Domazet, S., Lubura, M., Šušak-Lozanovska, I., & Ilik, N. (2021). Chinese social credit system: New challenges for the right to privacy? *Journal of Liberty and International Affairs*, *7*(3), 136–148. DOI: 10.47305/JLIA21371136d
8. Domazet, S., & Skakavac, Z. (2018). Skandal 'Cambridge analytica' – Novi izazov u zaštiti podataka o ličnosti? [Scandal 'Cambridge analytica' – A new challenge in the protection of personal data?]. *Srpska politička misao, 60*(2), pp. 115–133 DOI: https://doi.org/10.22182/spm.6022018.7

9. Gammeltoft-Hansen, T., & Vedsted-Hansen, J. (Eds.). (2017). *Human Rights and the Dark Side of Globalisation.* London & New York: Routledge
10. GAO. (2020). *Internet of Things: Information on use by federal agencies*. Downloaded 2024, April 15 from https://www.gao.gov/products/gao-20-577
11. Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. London: Transworld
12. European Parliament. (2023). *Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework* (2023/2501(RSP)). Downloaded 2024, January 5 from https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html
13. Fingas, J. (2018). *Beijing uses face-detecting smart locks to curb public housing abuses*. Downloaded 2024, May 2 from https://www.engadget.com/2018-12-31-beijing-facial-recognition-public-housing.html
14. Lau, T. (2019). *The government is expanding its social media surveillance capabilities*. Downloaded 2024, January 5 from https://www.brennancenter.org/our-work/analysis-opinion/government-expanding-its-social-media-surveillance-capabilities
15. Marković, D. M. (2019). Totalitarianism as a religious phenomenon. *Nauka i društvo*, *10*(2), pp. 5–20
16. Marković, D. M., & Dostić, S. (2019). McKinsey 7-S okvir implementacije strategije u oblasti bezbednosti [McKinsey 7-S framework for security strategy implementation] In: *Proceedings of the National scientific conference Contemporary Problems and Possible Solutions of Strategy and Strategic Management (SPSSM2019)* (pp. 159–176). Beograd: Fakultet za informacione tehnologije i inženjerstvo (FITI); Fakultet za poslovne studije i pravo (FPSP) Univerziteta „UNION – Nikola Tesla“
17. Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta* [*Criminal law regulation of computer crime*]. Novi Sad: Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu
18. Matijašević, J., & Ditrih, S. (2021). The impact of the Covid-19 pandemic on health and socio-economic factors in Serbia and the analysis of the legislative response of the state. *Pravo – teorija i praksa*, *38*(2), pp. 17–30. DOI:10.5937/ptp2102017M
19. Matijašević, J., & Dragojlović, J. (2021). Metodika otkrivanja krivičnih dela računarskog kriminaliteta [Methodology of detection of computer

crime offenses]. *Kultura polisa*, *18*(2), pp. 51–63. DOI:10.51738/Kpolisa2021.18.2p.1.04
20. Mladenov, M. (2023). Human vs. Artificial intelligence – EU's legal response. *Pravo – teorija i praksa*, *40*(1), pp. 32–43. DOI:10.5937/ptp2300032M
21. Newman, P. (2019). *Chinese officials are using smart devices for surveillance — including connected uniforms to track students*. Downloaded 2024, January 6 from https://www.businessinsider.com/chinese-government-smart-device-surveillance-2019-1
22. Page, C. (2021). *Is the UK government's new IoT cybersecurity bill fit for purpose?* Downloaded 2024, April 18 from https://techcrunch.com/2021/12/04/uk-internet-of-things-cybersecurity-bill/
23. Privacy International. (2020). *Mass surveillance* Downloaded 2024, April 15 from https://www.privacyinternational.org/learn/mass-surveillance
24. Satariano, A., Mozur, P., & Krolik, A. (2022). When Nokia pulled out of Russia, a vast surveillance system remained. New York Times [Online]. Downloaded 2024, May 2 from https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html
25. Schaer, C. (2023). AI-enhanced identification: A danger in the Middle East? *DW* [Online]. Downloaded 2024, May 2 from https://www.dw.com/en/ai-enhanced-identification-a-danger-in-the-middle-east/a-66602156
26. Skakavac, T. (2020). Uticaj društvenih mreža na pojavu maloletničke delinkvencije [Social networks and juvenile delinquency]. *Civitas*, *10*(1), pp. 72–93
27. United States Code. (1988). Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2711. Downloaded 2024, May 12 from https://www.loc.gov/item/uscode1988-007018121/
28. Verdict-Encrypt. (n.d.). *Edward Snowden: 'The problem isn't data protection; the problem is data collection'*. Downloaded 2024, May 3 from https://verdict-encrypt.nridigital.com/verdict_encrypt_winter19/edward_snowden_data_protection_collection_gdpr
29. Zirojević, M. & Ivanović, Z. (2021). *Cyber law – Serbia.* Belgrade: The Institute of Comparative Law