THE 10th ANNIVERSARY INTERNATIONAL SCIENTIFIC
PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- THE 10th ANNIVERSARY INTERNATIONAL FORUM
„SAFETY FOR THE FUTURE 2024" -
27th and 28th September 2024, Belgrade, Republic of Serbia

INTERNET OF THINGS AND THE RIGHT TO PRIVACY

Sinisa Domazet[1a]
[1] Metropolitan University, Faculty of Management, Tadeusa Koscuska 63, Belgrade, Republic of Serbia, sdomazetns@gmail.com

Received: 29th July 2024
Accepted: 19th August 2024

Original scientific paper

Abstract: *The dynamic development of information and communication technologies has led to the rapid development of the Internet of Things. Undoubtedly, the Internet of Things has brought numerous novelties in the functioning of modern man, but numerous challenges have also appeared in connection with these technologies. They relate to the protection of personal data, intellectual property rights, product liability, consumer rights and the like. The goal of the research in the paper is to analyze the relationship between the obligation to protect personal data and the Internet of Things, while pointing out the problems of misuse of data that have arisen through the use of modern technologies. The research established that numerous abuses were observed in practice regarding the application of technologies based on the Internet of Things. Normative method and legal-logical methods of induction and deduction were used in the paper.*

Keywords: *Law, Privacy, Internet of things, Security*

(Introductory lecture of the forum - work by invitation)

1. INTRODUCTION

The dynamic development of information and communication technologies has led to the rapid development of the Internet of Things (further: IoT). The Internet of Things is becoming more and more present in the everyday life of citizens, but also in the economy, in practically all areas. An increasing number of IoT abuse cases have been reported around the world, with serious consequences. Therefore, it should not be surprising that the governments of different countries are trying to cope with the increasingly diverse problems in the application of IoT, especially from the point of view of legal regulation. Legal regulation in this area is relatively poor, which is understandable considering that these are new technologies for which it is not possible to foresee all possible effects in application (positive or negative). Things are also complicated by the relatively complicated legislative procedure, which often slows down the process of passing relevant regulations, while in the meantime technologies advance.

[a] ORCID: 0000-0002-5964-2249

Undoubtedly, the Internet of Things has brought numerous novelties in the functioning of modern man, but numerous challenges have also appeared in connection with these technologies. They relate to the protection of personal data, intellectual property rights, product liability, consumer rights and the like.

The goal of the research in the paper is to analyze the relationship between the obligation to protect personal data and the Internet of Things, while pointing out the problems of misuse of data that have arisen through the use of modern technologies. First, the text will analyze statistical data regarding the Internet of Things, and then move on to the analysis of the relationship between the use of these technologies and the protection of personal data, using examples from practice.

2. STATISTICAL DATA REGARDING THE INTERNET OF THINGS

The Internet of Things is constantly growing, as evidenced by numerous statistics from various sources (Finance Online, IoT Analytics, FinleyUSA, European Commisiion, Statista, Tech Business News, Strategy Analytics, Crunchbase, Verdict, ARM, Tales Group, Telecoms.com), which show that the number of connected IoT devices is growing year by year and further growth is expected in the future.

According to the latest available data, there are approximately 14.76 billion connected IoT devices. The number of current IoT devices (14 billion) may seem staggering. But thanks 5G and other technologies, this figure is expected to grow almost 2x to 25.44 billion total IoT devices by 2030. There has been a notable shift from non-IoT devices to IoT devices over the last decade. In fact, by 2030, 75% of all devices are forecast to be IoT. The number of IoT platforms has increased year-over-year. In 2015, there were 260 publicly known IoT platforms. This figure jumped to 360 in 2016. And increased by a further 90 to 450 the following year. By 2019 there were 620 publicly known IoT platforms - 426 of which were still active in 2021 including global names like Microsoft and Amazon. In 2020, IoT spending reached $749 billion. In 2022, global IoT spending was predicted to hit $1 trillion. And in 2023, predicted spending rose to $1.1 trillion, continuing the increased rate of growth year-over-year. Despite a marked increase in IoT spending in recent years, market share by region isn't expected to change drastically. Back in 2018, the Asia Pacific region had the largest regional market share with 37% (over a third of total global IoT spending) (Howarth, 2024).

Video entertainment was the largest category of smart home spending in 2017 and 2018. Alongside IoT investment, IoT revenue is expected to grow year-over-year between 2019 and 2030. The IoT market is currently worth approximately $1.39 billion. And is expected to grow to almost $2.23 trillion at a CAGR of 12.57% by 2028. The single largest IoT revenue segment in 2022 was consumer media and internet devices ($101.8 billion). Connected vehicles ($73.8 billion) and payment terminals ($39.4 billion) were the second and third-highest IoT segments by revenue. Combined, they generated just over 10% more than consumer media and internet devices alone. In 2020, enterprise IoT comprised 76% of total IoT market revenue.That figure is expected to remain relatively steady, albeit falling to 73% in 2024 (Howarth, 2024).

Consumer spending on smart home-related devices worldwide increased by at least 12% year-over-year between 2015 and 2019. Unsurprisingly, during the height of the pandemic in 2020, smart home consumer spending dipped 9.47%. However, spending is expected to continue its upward trajectory through 2025, increasing year-over-year and peaking at $173 billion. Venture capital (VC) investment in the IoT space has rapidly increased in recent years. In the first half of 2021, the IoT space was responsible for 11.1% of all VC deals. That figure represents an increase of 1.2% over January-June 2020 and a further 2.8% over July-December of the same year (Howarth, 2024).

So, from the above data, it can be seen that the importance of IoT is growing, and thus many challenges arise in relation to the right to privacy and user protection.

3. THE NOTION OF THE INTERNET OF THINGS AND THE RIGHT TO PRIVACY

Considering all the complexity of the Internet of Things, it should not be surprising that the scientific and professional public cannot reach a consensus on a universal definition of this term. This is why one can encounter a wide variety of definitions and explanations (more or less comprehensive) that look at the Internet of Things from different angles. At this point, the definition from the Cambridge Dictionary should be mentioned, which defines IoT as “objects with computing devices in them that are able to connect to each other and exchange data using the internet” (Anon., 2016). According to the European Union Agency for Cyber Security, the Internet of Things is defined as “an advanced set of technologies and refers to a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context” (Anon., 2018). In the Chinese Ministry of Industry and Information Technology's "2011 IoT White Paper", IoT is characterized as "an expanded application of communication networks and the internet, which uses sensor technology and smart devices to perceive and recognize the physical world, and network connections to carry out calculations, processing, and data mining, in order to achieve information exchange and seamless connections between people and objects, or objects and objects. It reaches the goal of providing real-time control, precision management, and scientific decision-making vis-à-vis the physical world" (Chen, et al., 2018). As for the academic public, the definition of IoT given by Chen and Jin is interesting, according to which IoT represents "the network which can achieve interconnection of all things anywhere, anytime with complete awareness, reliable transmission, accurate control, intelligent processing and other characteristics by the supportive technologies, such as micro-sensors, RFID, wireless sensor network technology, intelligent embedded technologies, Internet technologies, integrated intelligent processing technology, nanotechnology" (Chen & Zhi-Gang, 2012).

Regarding the right to privacy, numerous definitions can also be found by the scientific and professional public, as well as by international organizations. The development of modern technologies has led to an increase in the scope of this term, so that it is no longer understood as simply as two centuries ago as "the right to be left alone", but in modern times some new features are added to it. That is why some authors also use the term "information privacy", which they mean "information security, which means that an individual in the information society decides when, to whom, how much and how to communicate personal data, taking into account their rights and needs, as well as rights and the needs of the community in which he lives. Information privacy unites the legal values of protection of the rights of individuals in the society of developed information technologies, and this concept of personal data protection, related to communication via electronic networks, is also called "e-privacy" (Boban, 2012). All in all, any definition of this term hits its core, and the emergence and development of IoT will undoubtedly further expand the scope of this term, given the numerous challenges it brings with it.

4. LEGAL CHALLENGES OF IoT IN RELATION TO THE RIGHT TO PRIVACY AND EXAMPLES OF ABUSE

Legal regulation regarding IoT is emerging and there is still no generally accepted regulation at the world level, except for a small number of countries that have already passed the appropriate regulation (US and UK for example). As far as the European Union is concerned, significant steps have been taken on this front, taking into account the numerous cyber-attacks faced by member state governments, the public and private sectors and citizens, as well as the

increasing damages that have been measured in billions of euros per year. It has been shown that cyber security in many areas is at an unsatisfactory level and legally unregulated, while at the same time the level of cyber security of products with digital elements is very low, with many vulnerabilities as well as rare and insufficient opportunities for updates to eliminate said vulnerabilities, and nothing a minor problem was not even with the information of buyers, that is, users of products who did not have detailed information about the cyber security of the products they buy, and therefore could not make appropriate decisions about the purchase or use of certain products. An additional problem is that there is an EU internal market, so there is a situation where a product is bought in one member state and used in other member states, or used outside the EU. Therefore, any cyber incident that may occur can automatically spill over into the entire internal market of the Union, due to the very nature of the IoT.

Because of all this, the EU institutions have decided to adopt appropriate regulations that will regulate these issues. Of course, the primary regulation that protects privacy is the GDPR, which was previously adopted by the institutions of the Union, which laid the foundations for the protection of personal data in the territory of the European Union. But the development of modern technologies and IoT required finding new solutions.

In this sense, we should mention the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, or Cyber Resilience Act (CRA) for short. Therefore, it is still a proposal for a regulation that is expected to enter into force in 2024.

By adopting this Regulation, the EU wanted to achieve four basic goals: (i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; (ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; (iii) enhance the transparency of security properties of products with digital elements, and (iv) enable businesses and consumers to use products with digital elements securely (European Union, 2022). The aforementioned Regulation regulates the following: rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity; essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes; rules on market surveillance and enforcement of the above-mentioned rules and requirements (European Union, 2022).

It is important to mention that the Regulation foresees corresponding obligations for producers. First, manufacturers must perform a risk assessment of a given product with digital elements in all phases of the product's life cycle, from planning and design to delivery and maintenance, according to the "essential requirements" from the Regulation. Products must ship without known exploitable vulnerabilities. The risk assessment must be clearly stated in the technical documentation, but also regularly updated during the period of customer support. Also, the manufacturer must ensure that the third-party components it incorporates into its products do not compromise the security of products with digital elements and must have appropriate policies and procedures, including coordinated vulnerability disclosure policies. It is also the manufacturer's obligation to notify the EU agency for cyber security (ENISA) of any exploited product vulnerability or incident within 24 hours of becoming aware of the vulnerability or incident.

The manufacturer is also obliged to provide effective support for at least 5 years for vulnerabilities during the life cycle of the product with digital elements, or during the expected life of the product, whichever is shorter. The manufacturer must monitor its products and adequately manage vulnerabilities, which includes their timely disclosure and publication of information about fixed vulnerabilities, taking adequate measures to facilitate the exchange of information about vulnerabilities and third-party components in that product, as well as other measures.

The provisions contained in Annex 1 of this act are particularly important, considering that they relate to the protection of personal data. In this regard, products with digital elements must (if applicable) among other things: ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems; protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms; protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions; process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimisation of data’); protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks; minimise their own negative impact on the availability of services provided by other devices or networks; be designed, developed and produced to limit attack surfaces, including external interfaces; be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques; provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions; ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users (European Union, 2022).

When it comes to practical examples of misuse of IoT before the proposal of the Regulation, the case that happened in Russia in 2013 should be mentioned first. Customs authorities there noticed that a number of consumer products originating in China, including electronic kettles and irons, were arriving with modifications that Russian authorities were not at all happy about. The devices contained hidden miniature Wi-Fi cards capable of spreading malware to any open Internet network within a radius of two hundred meters and could "telephone home" and transmit secret messages to China. Not only could these irons and kettles sneak onto your Wi-Fi network (which no one would expect from an everyday iron), but they could use your network to spread viruses to other computers in your home and send spam messages. your neighbors and the rest of the world (Goodman, 2017).

At this point, a case from 2017 can be mentioned, which illustrates how some IoT devices became the target of attacks and how this threatened the privacy of users. Namely, the company Vizio, the manufacturer of smart TVs, has reached an agreement with the Federal Trade Commission (FTC) in the USA in connection with the accusation of unauthorized collection and sharing of data about watching TV of users of its devices. The settlement included the payment of $2.2 million in damages and the company's obligation to allow users to choose whether they want the collected data to be shared with third parties in the future. The process of collecting TV viewing data was done through a feature called "Smart Interactivity" that was built into Vizio smart TVs. This feature was intended to provide personalized recommendations and ads to users based on their television viewing. However, the company collected and stored viewing data, including information about the programs and movies that users watched, without their prior notice or approval (Robson, 2017).

Also interesting is the 2019 US case involving Ring, where a number of users from several states who installed child monitoring cameras in the bedroom were exposed to hacking attacks and unusual activity on their cameras, which included and tracking users' activities without their consent. Apparently, the security of the Ring device was breached, giving hackers access to the cameras. A similar thing happened with Google's Nest and Taococo, baby monitors sold through Amazon, which also showed weaknesses regarding the protection of user privacy (Vigdor, 2019).

The mentioned few examples clearly indicate the wide range of threats that can occur due to misuse of the Internet of Things, as well as the serious consequences that can occur in these cases.

5. CONCLUSION

Considering the dynamic development of information and communication technologies, the Internet of Things will gain more and more importance. Its application in various fields shows positive things, but often the negative ones come to the fore. The above examples show that abuses related to IoT are increasingly present, with increasingly serious consequences. Undoubtedly, one of the most serious is the violation of the right to privacy, that is, various forms of misuse of personal data. The consequences and damages caused by the misuse of IoT are growing year by year and are in the billions of dollars every year. The analysis of statistical data from various sources confirms the stated position.

The aforementioned case (Vizio) raised the issue of data privacy related to smart TVs and highlighted the need to clearly inform users and ensure their consent regarding the collection and use of their personal data. In addition, there was a clear need to regulate the Internet of Things by legislative authorities, in order to protect the right to privacy in a more successful way.

Taking into account the above, some countries in the world have already adopted the appropriate legal regulation regulating the IoT. Examples are the USA and Great Britain. After a long consultation period, the European Union prepared and adopted the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, or Cyber Resilience Act (CRA) for short. With this act, an attempt was made to legally regulate products with digital elements, prescribing appropriate obligations for manufacturers in terms of preserving cyber security and the right to privacy.

At this moment, it is not possible to talk about the effects of the implementation of the Regulation, because it is still at the proposal level, but the cases that have been mentioned testify that the right to privacy will have to be protected more strictly in the future, especially when it comes to minors. A big problem will also be that the speed of legal regulation cannot keep up with the speed of development of modern technologies, especially IoT or artificial intelligence. The effects and scope of IoT at this moment are difficult to predict, and close coordination of legal experts and companies involved in IoT development will be necessary, so that the legal regulation is as consistent as possible with the latest technical and technological achievements, that is, so that the right to privacy is better protected.

REFERENCES

Anon., (2016). Cambridge Dictionary. s.l.:s.n.

Anon., (2018). ENISA. [Online] Available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot
[Accessed 17 July 2022].

Boban, M., (2012). The right to privacy and the right to access information in the modern information society. Collected papers of the Law Faculty of the University of Split, Volume 49, pp. 581-582.

Chen, J. et al., (2018). China's Internet of Things, Research Report Prepared on Behalf of the U.S.-China Economic and Security, Vienna: s.n.

Chen, X. & Zhi-Gang, J., (2012). Research on Key Technology and Applications for Internet of Things. Physics Procedia, Volume 33, pp. 561-566.

European Union, (2022). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels: s.n.

Goodman, M., (2017). Future Crimes. Serbian ed. Belgrade: Laguna.

Howarth, J., (2024). 80+ Amazing IoT Statistics (2024-2030). [Online] Available at: https://explodingtopics.com/blog/iot-stats [Accessed 15 July 2024].

Robson, W., (2017). Is Your TV Watching You? Vizio Busted for Spying on Customers. [Online] Available at: https://www.audioholics.com/editorials/is-your-tv-watching-you-vizio-busted-for-spying-on-customers
[Accessed 16 July 2024].

Vigdor, N., (2019). Somebody's Watching: Hackers Breach Ring Home Security Cameras. [Online] Available at: https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html [Accessed 16 July 2024].