Awareness of Croatian Citizens about the Advantages and Disadvantages of IoT Devices and Their Safety

P. Petrošanec, S. Čelan, R. Nikolić, M. Milenković
University of Zagreb, Faculty of Transport and Traffic Sciences, Zagreb, Croatia
paula.petrosanec44@gmail.com
0135265994@fpz.hr
robertina.zg@gmail.com
mmilenkovic@fpz.unizg.hr

Abstract - How knowledgeable are we about the Internet of Things? What do IoT devices mean to us in everyday life? The awareness of citizens of the Republic of Croatia will be discussed in this article on issues related to knowledge of IoT devices and their capabilities. For this paper, a survey has been conducted among the population between the ages of 19 and older on issues of familiarity with IoT devices, and an analysis of the responses was made. This paper shows how knowledgeable the citizens of the Republic of Croatia are about IoT devices, their capabilities, their security, and the possibility of omissions, data leaks, and violations of the GDPR, i.e., omissions with the sharing of their personal data. Considering that the global pandemic in the last two and a half years has stimulated computerization and the sudden expansion and ever-faster spread of IoT devices, the familiarity of EU citizens and knowledge about their capabilities has been called into question. There is also a viable need for educating and familiarizing the citizens of the Republic of Croatia with the capabilities of IoT devices and their advantages and disadvantages. This paper discusses the theoretical and practical implications of the research and gives recommendations for further research.

The key words: Internet of things, IoT devices, security, digital transformation, data privacy

I. INTRODUCTION

IoT or Internet of Things stands for a network of connected devices that has constant (24/7) access to the Internet, to exchange data with other smart devices, and holds software support that enables usage without human help.

The idea of connecting and implementing sensors to various devices appeared already in the eighties (of the 20th century), although such ideas existed in different forms much earlier [1]. John Romkey developed the first IoT device in 1990. It was a toaster that was turned on and off via the Internet [2].

The IoT primarily includes smart mobile phones, smart TV, tablets, smart watches, smart electric meters, smart lighting, smart monitoring systems, smart refrigerators, smart ovens, smart virtual personal assistants, smart heating and cooling systems, and many other different smart devices. The purpose of IoT devices is to collect data from end users and share their information to facilitate and simplify their daily life processes, i.e., their daily activities. IoT devices make it easier for users to perform everyday tasks. This paper will address the numerous advantages and disadvantages.

Users share their personal data with various third parties without knowing with whom their personal data have been shared. It is important to note; when purchasing an IoT device, end users do not sign the consent for sharing of their data, which is prescribed by the GDPR[1].

According to Ericsson research [3], there will be 22 billion devices of IoT devices by the end of 2023, and 24 billion by 2050, which indicates a significant growth of IoT devices in the next 25 years.

While Business Insider experts expect that figure to grow to 30.9 billion by 2025. [4] As the number of IoT devices increases, so does the attack surface of the cybersecurity vulnerabilities they present. More than one billion IoT attacks occurred just during 2021, of which almost 900 million were phishing attacks [5].

II. METHODOLOGY

For this paper, a quantitative questionnaire was conducted on a sample of 504 citizens/respondents from the Republic of Croatia (further: Croatia). The aim was to analyze their familiarity with the capabilities of IoT devices.

For this research, it was used a questionnaire as a data collection tool. Web-Assisted Interviewing (WAI collected the data) [6] since WAIs are easier, more efficient, and usually conducted without expenses with

[1] The basic requirements for the effectiveness of valid legal consent are defined in Article 7 and additionally stated in the introductory statement 32 of the GDPR. Consent must be freely given, concrete, transparent, informed, and unambiguous. To obtain freely given consent, it must be given on a voluntary basis. Inherently, it implies a real choice of the data subject. GDPR:EU, https://gdpr.eu/gdpr-consent-requirements/, (Accessed: 15th of February 2023)

less error occurrence, than paper questionnaires and some other types of surveys [6]. The authors have opted for ‘’Mixed-mode design with a choice of completion method’’ [6], which is used among different methods, such as web, phone, or mail, within the groups of respondents who have a connection with the University (mostly students and professors). Due to the predicted large number of respondents and its cost-effectiveness, this type of method was chosen. Data were collected from the 12th of December 2022 until the 15th of January 2023, and the questionnaire was provided in an Internet-only version via Google Forms.

The questionnaire was provided to participants using social media, such as Viber, WhatsApp, Facebook, Signal, and Telegram. The questionnaire was conducted anonymously, and the Croatian language was used.

It contained of ten (10) questions. The first question was concerning the age of the respondents. The authors decided not to ask any personal data of respondents except the age, because information is irrelevant for the meaning of the answers. The second question asked the respondents if they know of IoT devices. There were only two (2) answers available: „Yes’’ and „No’’. The third and the fourth questions were about the knowledge of respondents on IoT devices to selected from the multiple answers. Thus, respondents could also add their own answer/s. The questions also offered incorrect answers to reveal the real knowledge of the respondents.

With the fifth and sixth questions, it was attempted to examine the awareness of the security of IoT devices and the possibility of cyber-attacks via them. The seventh and eight questions included awareness and accessible education that the citizens already have in Croatia (in everyday life, examples on TV, radio, Internet, schooling system of the Republic of Croatia, etc.). The final two (2) questions examined the personal opinions of respondents about the improvement of their life by using IoT devices and whether they plan to acquire such a device soon.

All the questions from the questionnaire made it possible to check the sufficient familiarity of the citizens of Croatia with the capabilities of this type of device. Therefore, the paper offers suggestions and clarifications on different forms of education for citizens of all ages.

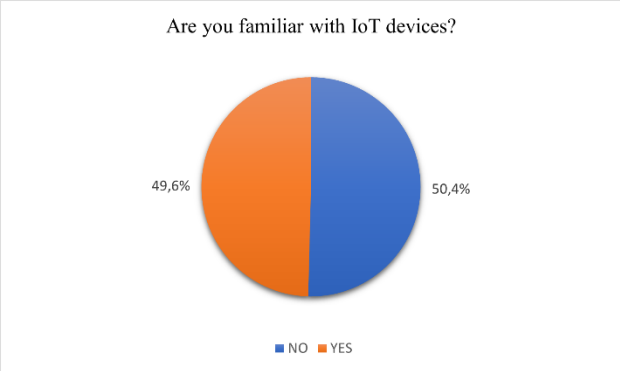

Figure 1: Question: Are you familiar with IoT devices?

III. ANALYSIS OF THE RESULTS

The questionnaire was completed by a total of 504 respondents. The first question showed the age of the respondents. 65.8% are 19 to 25 years old; 5.4% are 26 to 31 years old; 4.8% are 32 to 37 years old; 4.4% are 38 to 43 years old; 7.2% are 44 to 49 years old, and there are 12.5% of the respondents older than 50 years of age.

The second question gave an insight into the percentage of respondents’ familiarity with IoT devices. According to *Figure 1*, 49.6% of respondents are acquainted with IoT devices, and 50.4% of respondents were not acquainted with IoT devices. It is worrying to know that a large number of respondents are not familiar with IoT devices, especially when the largest percentage of respondents are young people under 25 years old.

The third question included 482 respondents. 411 respondents (85.3%) know that a TV can be a smart IoT device. 264 respondents (54.8%) are familiar with the fact that the heating system can be organized as a smart IoT system, while 224 respondents (46.5%) believe that an electric meter could also be a smart IoT device. In the same question, devices that are not IoT devices were specifically listed, and a certain number of respondents also included these devices as IoT devices, see *Figure 2*. As an example, a mixer was given, and as many as 87 respondents (15%) concluded that it could also be an IoT device.

From the answer to question 4, it is evident that 374 respondents (74.9%) own a smart TV, whereas 86 respondents (17.2%) do not have any aforementioned IoT device in their households. Under "other", the respondents added some of the smart devices they own, such as: a smart vacuum cleaner, a power socket, a smartwatch, a smart bracelet etc. The question arises whether the respondents can recognize which IoT devices they have in their household.

The fifth question, 243 respondents (49.8%) answered that IoT devices are unreliable, whereas 245 respondents (50.2%) replayed that they are reliable. Furthermore, out of 491 respondents to the sixth question, only 14 respondents (2.9%) replayed that their data is not exposed to potential threats on the Internet, while 277 respondents (56.4%) answered that their data is somewhat exposed to threats, and 200 respondents (40.7%) are aware of the dangers that can happen with their personal data on the Internet (See *Figure 5*).

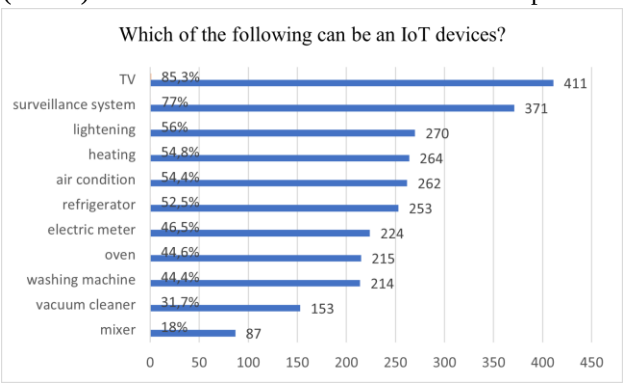

Figure 2: Question: Which of the following can be an IoT device?

In the seventh question: "Do you think that you are sufficiently knowledgeable about the capabilities of IoT devices?", 148 respondents (30.3%) answered that they are not at all knowledgeable about the possibilities that IoT devices bring.

As many as 253 respondents (51.7%) believe that they are not sufficiently knowledgeable about the operation of IoT devices and their capabilities. Only 88 respondents (18%) believe that they have sufficient knowledge about the capabilities of IoT devices. From the given answers, it can be concluded that over 80% of the respondents believe that they are not sufficiently educated about the possibilities of IoT devices.

On the 8th question, as many as 187 respondents (42.3%) answered that adequate education on IoT devices is not provided, and only six (6) respondents (1.4%) believe that education in Croatia provides sufficient education on IoT devices. All other respondents are not satisfied with education on IoT devices in the Croatian educational system (See *Figure 3*).

Out of the 476 responses we received from the answers in question nine (9), the majority of respondents believe that IoT devices and their use do not contribute to improvements to the quality of their life. In the last question, only 485 respondents answered this question while 292 respondents (60.2%) do not plan to buy an IoT device in the next year, whereas 193 respondents (9.8%) concluded that they plan to buy a smart IoT device in the next year. (See *Figure 4*)

On the basis of the questionnaire, a relatively insufficient percentage of respondents who stated that are familiar with the technology of IoT devices was revealed, and the above indicates, or may indicate, one or more of the following:

a) according to the answers to the seventh question, only 18% of respondents consider that they are sufficiently knowledgeable about IoT devices, which is insufficient for the entire Croatian system;

b) The Croatian executive state and local authorities have not regulated the introduction of IoT devices into the Croatian education system for pupils and students, or for adults through forms of lifelong learning, and they have no plans of implementing such solutions;

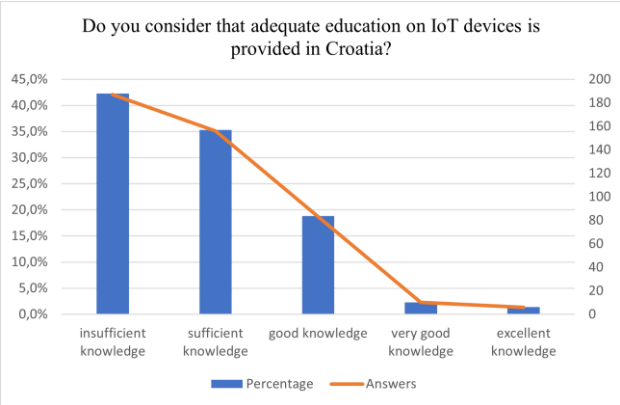

Figure 3: Question: Do you consider that adequate education on IoT devices is provided in Croatia?

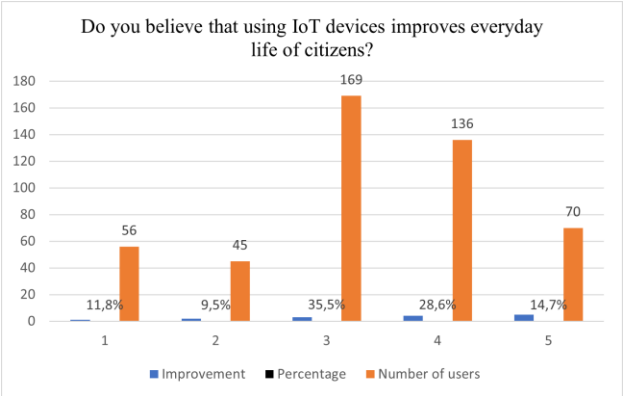

Figure 4: Question: Do you believe that using IoT devices improves the everyday life of citizens?

c) the Croatian education system does not contain the necessary education about IoT devices, i.e., about today's leading technology.

IV. LEGAL REGULATION OF IOT DEVICES IN EU AND CROATIA AND SUGGESTIONS FOR AMENDMENTS IN PRACTICE

A. Legal aspects of the security of IoT devices

The European general data protection framework, the General Data Protection Regulation (further: GDPR), does not explicitly mention IoT devices, as well as Croatian national laws, such as the Croatian Act on the Implementation of the General Data Protection Regulation [7], which contains a series of introductory statements and provisions applicable to data collection through smart home devices and the Internet of Things.

IoT products and services enable the collection of large amounts of data, some of which may be potentially sensitive. It is necessary to take protective measures, but it's important not to jeopardize the privacy of users.

The GDPR [8] requires that the service provider ensures the safety and security of the processing. It considers this further in the introductory statement 39, elaborating the principles of data protection, especially the principles of purpose limitation, storage limitation, and data minimization: "Natural persons should be aware of the risks, rules, protective measures, and rights related to the processing of personal data and how to exercise their rights related to such processing. Personal data should be adequate, relevant, and limited to what is necessary for

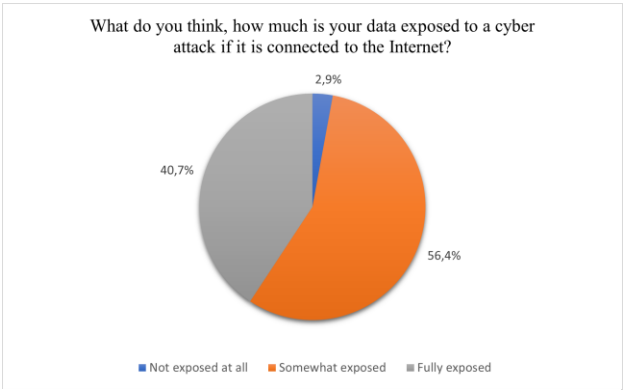

Figure 5: Question: What do you think, how much is your data exposed to a cyber-attack if it is connected to the Internet?

the purposes for which they are processed. In particular, this requires ensuring that the period for which personal data is stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing cannot reasonably be fulfilled by other means."

Hence, the results in *Figure 5* show that Croatian citizens are not familiar with the risks of trading with their personal data and the dangers they bring. As Vojković et alli mentioned: "Users should be aware of what data is being collected about them. The problem is that many IoT devices do not have high-quality protection. Consumers must be aware of this, which is not within the scope of GDPR, but consumer protection regulations." [9] The security threats posed by IoT devices have already been described in the literature. [10]

In parallel with the exponential growth of technology, the number of various directives, regulations, and standards in the field of security is growing.

The European Union Agency for Cybersecurity (ENISA) in its tasks regarding IoT and security highlights:

• Promoting harmonization of IoT security initiatives and regulations,

• Raising awareness of the need for cyber security in IoT,

• Defining the security guidelines of the software and hardware development life cycle for IoT,

• Achieving consensus for interoperability in the IoT ecosystem,

• Encouraging economic and administrative incentives for IoT security,

• Establishing secure life cycle management of IoT products/services,

• Clarification of responsibilities among IoT stakeholders.[11] [12]

According to Vojković et alli, [13]; the general legal obligation for the cybersecurity of IoT products in the EU does not exist in the EU, hence, it is incompatible with the obligation of the EU to provide for a higher level of consumer protection, as mentioned in Article 169 [14] of the Treaty of the Functioning of the European Union.

New functionality brings new data security and privacy challenges; experts noticed that the weakest links of IoT can be driven by the low-cost devices with low-security and cryptography technologies.[15]

B. Practical methods of citizen education

Education about the security of IoT devices should start from the preschool age in such a way as to create and conduct workshops. Specifically, education about IoT devices through practical classes would be introduced into the preschool curriculum.

The classes would include knowledge about threats that appear during the use of devices (e.g., mobile phones, tablets, and computers). By using this approach, it is important to raise the awareness of potential dangers that children do not understand due to their age.

Adequate lectures on IoT devices and their security should be added to the elementary and secondary school curriculum as part of computer science classes.

To ensure the education of all students in this area, it is necessary to conduct a lecture by an expert (e.g., a professor of Computer Science) at least once a year during the class community hour.

It is also important to conduct workshops and lectures on the presented topic with the faculties.

For the elderly, the local self-government should engage experts who would provide education through workshops on the dangers of their personal data, as well as their rights. In addition to workshops, it is necessary to apply education in the media through advertisements, newspapers, and magazines financed by the Government, and to obey the EU regulations and directive articles.

Additionally, ENISA has regulated the basic guaranteed level with the European cybersecurity certificate or EU declaration of conformity, which provides a guarantee that ICT products, ICT services, and processes for which that certificate has been issued, meet the appropriate security requirements. [14]

The same includes security functionalities, testing whether the products have undergone evaluation, the purpose of which is to minimize known basic risks for incidents and cyberattacks, but it is not currently implemented in practice because manufacturers do not follow the recommendations made.

Therefore, the evaluation activities that would necessarily be undertaken should include the following: review to prove the absence of publicly known vulnerabilities and testing to prove that ICT products, ICT services, or ICT processes correctly apply the necessary security functionalities.[16]

The lack of foresight is not the only IoT security issue facing newly digital industries. Another major issue related to IoT security is the technical resource limitations of these devices.[17]

IoT technology has posed new security challenges that go beyond traditional data security due to the unique multi-layered network and nature of the IoT architecture used. IoT security is challenging due to its interaction between physical and digital components. Additionally, the environment of the IoT business model, with both its regularity and contractual obligations and the liability requirements themselves, represent one of the key areas that calls for answers.[18]

Therefore, this paper shows how IoT devices pose a greater risk to personal data than previous surveillance technologies.

V. CONCLUSION

This paper aims to analyze citizens' familiarity with the capabilities of IoT devices.

It also discusses the possibility of introducing education into the entire schooling system in Croatia, starting from an early age. It is necessary to inform all respondents i.e., all users of IoT devices, regardless of age, about their existence, capabilities, possibilities, advantages, and

disadvantages, as well as about the dangers of using their personal data without their knowledge.

This paper aims to raise awareness of the need to apply and improve the legal framework in the the 27 Member States.

The idea behind this paper was to test the research hypotheses and to use the results of this questionnaire in future practice.

From the answers of the respondents can be concluded that the citizens are not familiar with the technology of IoT devices. However, they know that the system in Croatia does not provide adequate education and that the manufacturers do not inform users about the potential risks of devices of this type. This indicates necessity to introduce additional stricter regulations at the level of the European Union so that manufacturers must meet certain standards, while not setting them according to their interests.

Starting with harmonizing and complying with current regulations and recommendations, as well as obliging manufacturers to apply the same in practice.

It is necessary to raise the citizens' awareness that the use of such devices makes the life of an individual easier, but at the cost of taking away their privacy.

According to the questionnaire, respondents have no problem providing personal information about their lives, but they want to be sure that this information will not be used for any other purpose.

The security of the Internet of Things is mostly the responsibility of the manufacturers themselves, who should bear the possible consequences caused by the compromise of systems. [19]

In sum, Croatia needs a fundamental shift when we think of education concerning the IoT devices. We highly recommend the adoption of a national-level strategy for better citizen inclusion in joint decision-making processes regarding the implementation of IoT technology.

Certainly, it is expected that with the further rapid growth of IoT development, adequate and regular and up-to-date education of all citizens will be needed. It will grow human consciousness, and for this very reason, it is necessary to decrease incorrect maintenance.

Ultimately, with the growing technology, the number of security vulnerabilities and data breaches will also increase; therefore, this research continues through another paper on the education and protection of the security of IoT devices.

REFERENCES

[1] Omegasoftware, '' Internet of Things – Begginers Guide'', 2021, https://www.omega-software.hr/internet-of-things-vodic-za-pocetnike/, [Accessed 1st of February 2023]

[2] D. Šipek, DuplicoIT, ''What is IoT or Internet of Things?'', 2022, https://duplico.io/sto-je-iot-ili-internet-of-things/, [Accessed 1st of February 2023]

[3] Ericsson.com, IoT's potential, https://www.ericsson.com/en/internet-of-things, [Accessed 20th of February 2023]

[4] A. Husar, IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities, 2022 https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities, [Accessed 20th of February 2023]

[5] N. Liebermann, SAM Seamless Network, '' 2021 IoT Security Landscape'', 2022, [Accessed 1st of February 2023]

[6] N. Bradburn, S. Sudman, B. Wiansink, Asking questions : the definitive guide to questionnaire design—for market research, political polls, and social and health questionnaires, John Wiley& Sons, 2004, pp. 303-304.

[7] Croatian Act on implementation of the General Regulation on Data Protection, Narodne Novine, NN 42/2018, (Narodne Novine are an Official Gazette of Republic of Croatia).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, preamble 39, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HR, [Accessed: 20th of February 2023]

[9] G. Vojković, M. Milenković, T. Katulić, IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law, Business Systems Research | Vol. 11 No. 3 |2020, p. 168.

[10] Jurcut, A., Niculcea, T., Ranaweera, P., & LeKhac, A. (2020), "Security considerations for Internet of Things: A survey". SN Computer Science, Vol. 1, Article 193.

[11] ENISA, GUIDELINES FOR SECURING THE INTERNET OF THINGS, Secure supply chain for IoT, 2020, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things (Accessed: 20th of February 2023)

[12] Versoaltima.com, IoT and Cyber Security Challenges, 2022, https://www.versoaltima.com/wp-content/uploads/2019/11/IOT-IGOR-GREGUREC.pdf, (Accessed: 21st of February 2023)

[13] Vojković, G. & Milenković, M. (2021) Liability for Early Safety Obsolescence of IoT Devices due to Information Security Reasons. U: Skala, K. (ur.)MIPRO 2021 44th International Convention Proceedings doi:10.23919/MIPRO52101.2021.9596674

[14] Consolidated version of the Treaty on the Functioning of the European Union,Article 169, *OJ C 202*, In force, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016E169, (Accessed 20th of February 2023

[15] Vongsingthong S., Smanchat, S. (2015), "Review of data management in Internet of Things", Asia-Pacific Journal of Science and Technology, Vol. 20 No. 2, pp. 215-240

[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (Cybersecurity Act), SL L 151, Art. 5 and 6, In force, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG, (Accessed: 21st of February 2023)

[17] S. Shea, Tech Target, IoT Agenda, 2022, https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security, (Accessed 21st of February 2023)

[18] A. M. Awadelkarim Mohamed and Y. Abdallah M. Hamad, "IoT Security: Review and Future Directions for Protection Models," *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, Tabuk, Saudi Arabia, 2020, pp. 1-4, doi: 10.1109/ICCIT-144147971.2020.9213715.

[19] Cert.hr, Security of Internet of Things, 2023, https://www.cert.hr/sigurnost-interneta-stvari-iot/, (Accessed 20th of February 2023.)

APPENDIX - Questionaire

1. U koju dobnu skupinu pripadate?
2. Jeste li čuli za IoT uređaje?
3. Koji od navedenih mogu biti IoT uređaji?
4. Posjedujete li koji od navedenih pametnih uređaja?

5. Smatrate li da su IoT uređaji pouzdani za sigurnost vaših osobnih podataka?

6. Što mislite, koliko su Vaši podaci izloženi cyber napadu ukoliko su povezani na internet?

7. Smatrate li da ste dovoljno upućeni u sposobnost IoT uređaja?

8. Smatrate li da se u RH pruža adekvatna edukacija o IoT uređajima? 1 označava najmanju upućenost, a 5 najveću.

9. Smatrate li da korištenje IoT uređaja unapređuje svakodnevni život korisnika? 1 označava najmanji napredak, a 5 najveći.

10. Planirate li u idućih godinu dana kupiti IoT uređaj?