The Smart Campus Conflict: Security vs Privacy? A Pilot Study among Estonian Students

Kate-Riin Kont

kate-riin.kont@sisekaitse.ee

Estonian Academy of Security Sciences

ICDS 2025

May 18, 2025 to May 22, 2025 - Nice, France

- Graduated from the Department of Librarianship and Information Science, Tallinn University in 1995.
- Earned a MA from the same department in 2004.
- Defended Doctor of Philosophy degree at the Institute of Digital Technologies in Tallinn University in 2022.
- After worked in librarianship for 30 years and since 2017 also as a lecturer at Tallinn Health Care College, I started my work as a researcher in Estonian Academy of Security Sciences, Internal Security Department, in 2022.
- Research area is cybersecurity, especially cyber and information security of public sector organizations and its connection to the human factor, as well as technological developments in Internet of Things devices and the specifics and security of its various application areas.
- My research topics are based on the principle that Estonia's security begins with the activities and readiness of each individual, and cyber protection begins with the individual sitting behind the Computer screen and the person's skills, knowledge, beahviour and attitude.

Dr. Kate-Riin Kont
Estonian Academy of Security Sciences

Importance of the topic

- In recent years, the concept of a smart university campus has attracted a lot of attention. A campus can be considered a small City that serves different user groups and offers various services.
- An integral part of this concept is technological applications of the Internet of Things, the implementation of which is inevitable in the development of smart solutions.
- In the case of smart technology, it is important that ethical, social, privacy and security considerations are paid attention to simultaneously with technological development. Our willingness to share data about ourselves is changing and evolving over time.

Importance of the topic

- Campus is a place where faculty and students spend a large part of their day, but often also at night (dormitories). Living and studying in campus brings its own challenges, as risks that need to be mitigated can arise in environments filled with human activity.
- Maximising safety and security in today's higher education institutions und oubtedly presents enormous challenges.
- Since the 1980s, concerns about campus crime and student safety have grown (Jennings et al., 2007). Campus safety has become a global concern, particularly in light of the mass shootings and other serious crimes that have occurred in college communities in the United States and elsewhere. Whether the campus is located in a metropolitan or rural area, a significant number of people feel unsafe on campus at evenings. Student-related crimes account for approximately 80% of all crimes reported on college campuses.

The purpose of the study

- Campus safety surveys have measured perceptions of safety by asking respondents about their feelings of safety by time of day and location (Jennings et al. 2007; Maier and DePrince 2020), in buildings on campus, in dormitories (Shariati and Guerette, 2020), in areas near the campus, in parking lots, and garages. Schafer et al. (2018, p. 319) measured perceptions of campus safety by asking students whether they support campus safety and security policies and observed that “there is little research on how students perceive policies designed to ensure their safety.”
- A pilot survey was executed to gain an initial understanding of what is important to Estonian students as the main “users” of the campus in terms of security and privacy. Are Estonian university students willing to give up some of their privacy for the sake of their physical safety? Do they trust their university’s information security systems enough to be sure that their data and daily movement routine on campus will not be leaked to criminals or that the integrity of the context of the data collected about them will not be violated? Are they confident that the data collected from them is protected from data leaks related to cyberattacks and is handled ethically?

The concept of a safe campus

- The creation of a safe space originated in America, where the concept of CPTED (Crime Prevention through Environmental Design) was introduced. The first to use this concept was American criminologist C. Ray Jeffery in 1971, who wrote: “Crime can be controlled through urban planning, in which safety and security are planned into streets, buildings and parks. Our cities are unsafe because they provide opportunities for crime. However, cities can also be planned in a way that increases close contact between people” (Jeffery, 1971, p. 598).
- A safe city is a city that, by integrating technology and the natural environment, increases the effectiveness of safety processes to reduce the risk of crime and terrorism, enable its citizens to live in a healthy environment and have easy access to healthcare, and achieve preparedness and rapid response to imminent or emerging emergencies (Lacinák and Ristvej, 2017). A safe city is also defined as a liveable city that focuses on the problem of crime in urban areas and whose concept is the creation of a unified response plan for major emergencies (Aris-Anuar et al., 2011; Vitalij et al., 2017).
- One of the main challenges in developing smart cities is the processing and management of data, as well as the linking of data with new systems and sensors in the smart city that affect security and privacy (van Zoonen, 2016). The threats arising from information security, data privacy and cyber-impact factors, where unauthorised access to information can lead to unintended consequences, highlight the importance of addressing these issues already at the planning and development stage of smart cities (Elmaghraby and Losavio 2014).

The concepts „security“ and „privacy“

- Security is related to data protection, while privacy is related to the protection of a user’s identity. Security refers to the protection of data from unauthorised access. Every organisation implements security measures to limit who has access to such information. When data that was supposed to remain confidential falls into the wrong hands, unpredictable things can happen.
- One of the most important factors to address when implementing smart technology is privacy. Privacy can best be defined as freedom from intrusion by others into one’s personal life or possessions. Privacy and security are related topics but are not synonymous: information security aims to protect sensitive information from anyone who does not have appropriate access to it, while privacy is more of a person-centered concept related to an individual’s preferences regarding the treatment of information about them (Azad, 2008; Romdhani, 2017).
- Privacy ensures that individuals have control over the information they disclose in the context of a specific application (e.g., the Internet). Ensuring privacy means that personal data disclosed to specific entities for a specific purpose is not made available to other unauthorised entities or used to obtain additional information. Security is related to data. The relationship between security and privacy is that security is necessary, but not sufficient to protect privacy. In fact, any violation of security properties, especially data confidentiality, directly affects privacy.

The data collection method

- The data used in this paper is based on an overview of relevant literature, highlighting and explaining the concepts of “security and privacy”.
- The data collection method was the online questionnaire distributed among Estonian public universities and universities of applied sciences. A total of 286 students from all over Estonia answered the questionnaire.
- A five-point Likert scale questionnaire was used as the methodology of the study. Since the opinions of students in the context of a “smart campus security and privacy” have not been studied before in Estonia, open questions were considered necessary to add to get broader feedback on a field that has been little studied or not at all.
- The results are interpreted based on the literature, and data obtained from the completed questionnaires were analysed using Excel’s Data Analysis ToolPak. The results are presented mostly as tables and bar charts. The examples of open answers give added value.

Results: Physical security is ensured by technological solutions and privacy

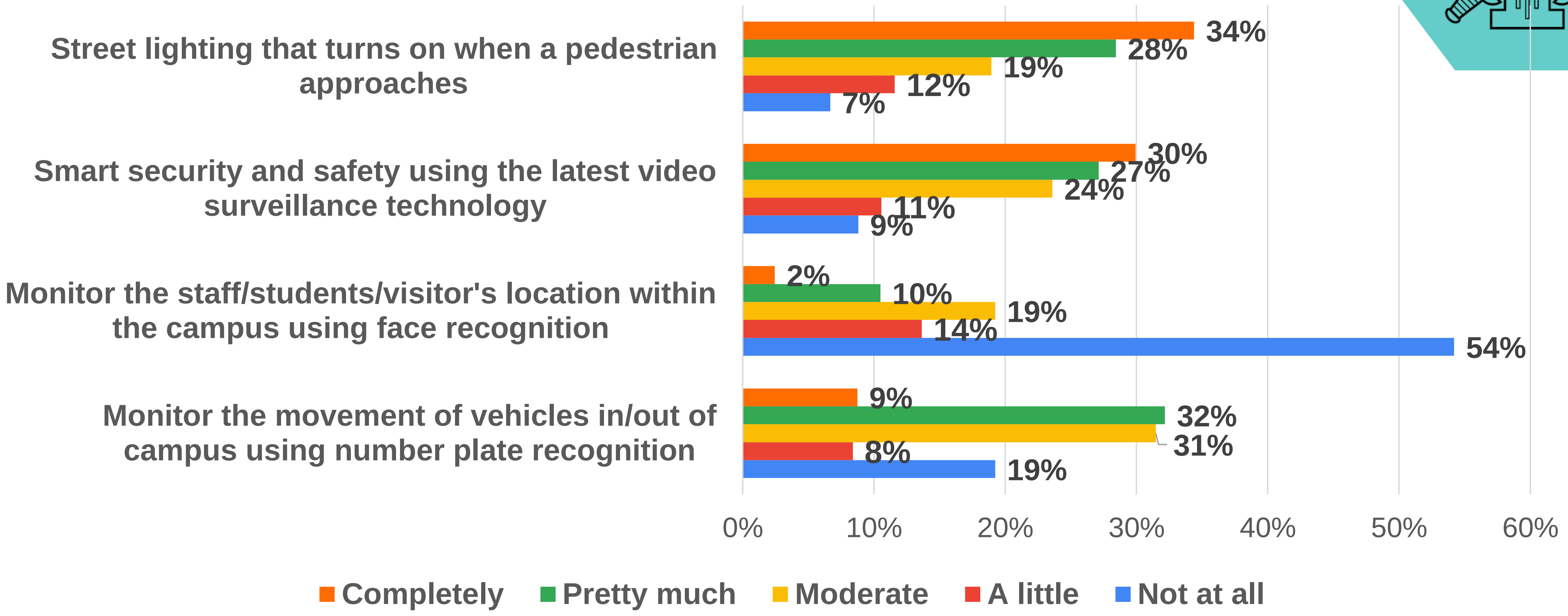

Figure 1. The importance of having technological applications that ensure physical security

Results: Technological solutions as supporters of physical and cyber security

Table 1. Technological solutions as security enablers

Technological solution:	Strongly disagree	Somewhat disagree	Neither agree	Somewhat agree	Strongly agree
The campus must have protection against cyber attacks	0%	1%	2%	17%	80%
The campus has protocols in place to prevent and manage every kind of risk and disaster	1%	3%	16%	34%	46%
The campus ensures my physical safety	4%	4%	14%	30%	48%
The campus has technological systems supporting security (e.g., facial recognition system)	20%	18%	26%	23%	13%
Average	6%	6%	14%	26%	48%

Results: Sensors with various monitoring functions as security supporters

Table 2. Sensors with various functions for security and support

Would you agree to have sensors installed on your campus:	Strongly disagree	Somewhat disagree	Neither agree	Somewhat agree	Strongly agree
For surveillance/security purposes	10%	15%	13%	30%	32%
For the purpose of monitoring the movement of students and their visitors – face recognition	43%	24%	13%	12%	8%
For the purpose of vehicle monitoring – number plate recognition	18%	21%	19%	26%	16%
For the purpose of monitoring environmental variables to improve energy efficiency	7%	12%	12%	24%	45%
When using IoT/RFID for navigation	10%	13%	41%	19%	17%
AVERAGE	18%	16%	20%	22%	24%

Results: Collection, storage, protection and privacy of personal data

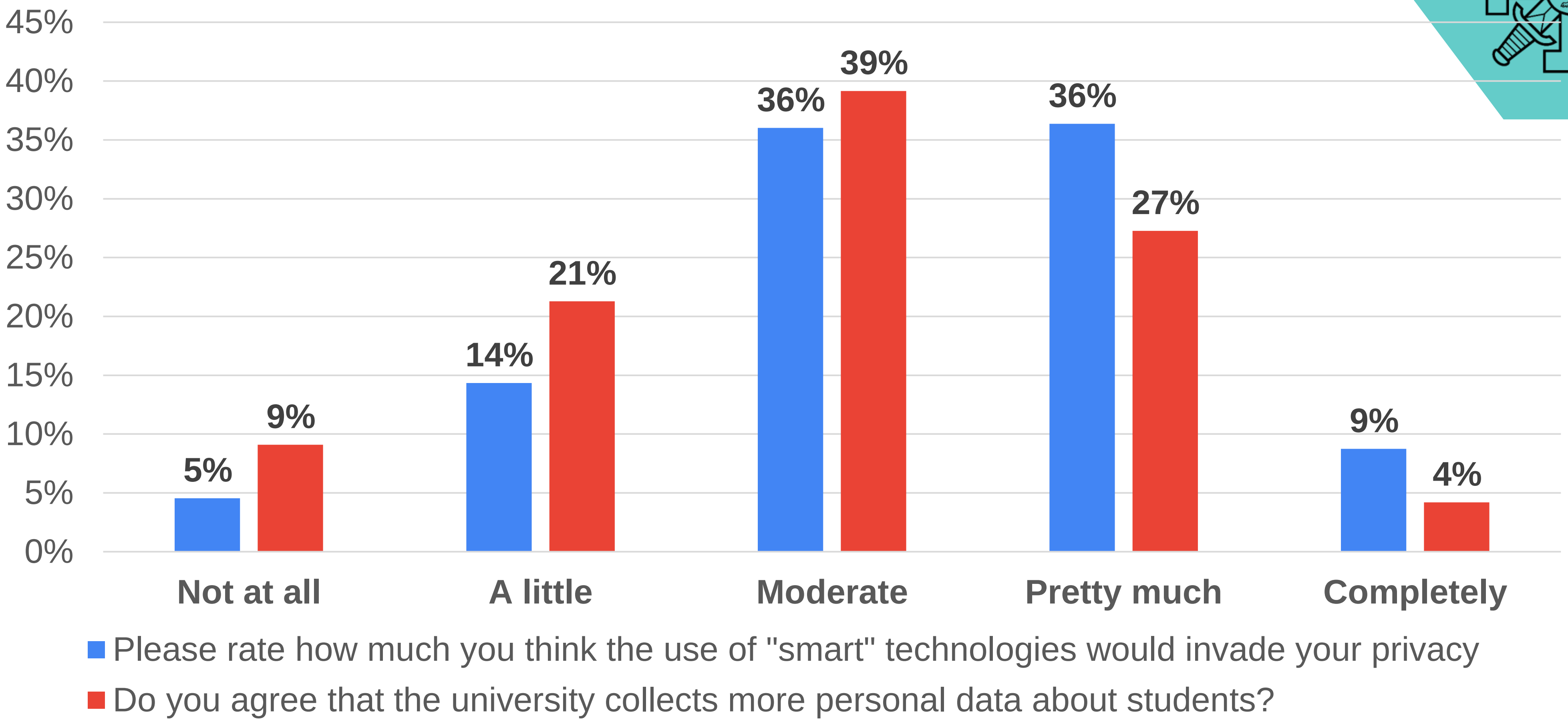

Figure 2. Respondents' opinion on the extent to which "smart" technologies and the collection of more personal data would interfere with their privacy

Results: Collection, storage, protection and privacy of personal data

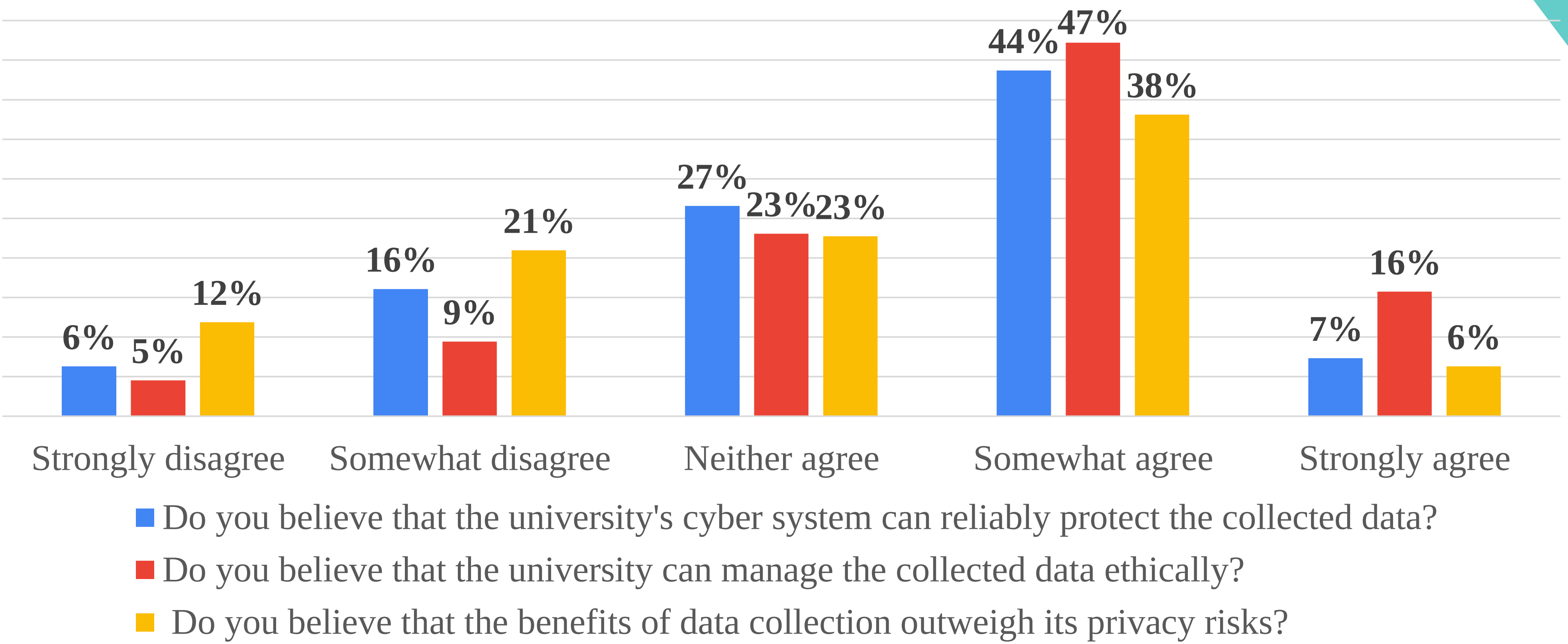

Figure 3. Respondents' assessments of the potential responsibility of higher education institutions in protecting the privacy of their members

Respondents’ comments

- *I would recommend getting together a team and really going over each of the proposed features and thinking about the implementation and data collection. Do you really need face tracking to identify each student, maybe a broader mobility analysis which looks at the number of people entering/exiting is enough? Maybe you can do anonymised tracking via cameras as well.*
- *I think the problem is not the loss/absence of privacy when introducing facial recognition and other security systems. It’s where they are installed and how the information is used. And the transparency of this entire process and clear communication between students and the university.*
- *There are two very different topics here that should be probably discussed separately – firstly the “smart” solutions and their pros and cons and secondly the ethical issues when using private information*.
- *People are irrational and have a natural tendency (for evolutionary reasons) to maximise their safety at all costs. But rationally, we already live in a very safe (and convenient) environment and every improvement in these areas costs a lot in either freedom or privacy. We already live in a world where keeping control over our data is very difficult. Even in a public space, you can’t go out without being filmed by plenty of cameras (just try to pay attention to it for a few days, and you will see). While it’s certain that “smart” cities and campuses can bring convenience and improve the efficiency of these places, it’s important to: 1) accurately estimate the impact on privacy, 2) always be completely transparent about the collected data, and 3) give people an option to opt out of as much data collection as possible. Thank you for taking these into account.*

Respondents’ comments

- *Nobody in history has been able to protect their data. The biggest names in tech, with valuations exceeding the annual budgets of entire governments (for several YEARS, no less), have had breaches and leaks. The more data you collect, the bigger a target you are.*
- *Cybersecurity is an essential part of any online interaction these days, and investing in its protection should not be a waste. It is impossible to predict every event or crisis, much less plan for them all, so it should only cover the most likely scenarios and leave room for improvisation for the less likely. Physical safety is important because students need to feel safe to learn to the best of their ability. That said, I don’t think physical safety is too big of an issue right now. Any security system needs to be supported with resources to make it work, but I think, as already stated, there needs to be a broader discussion with the faculty and student body about their willingness to participate in such a system.*
- *The technologies used should be introduced to students and they should give their permission to use it on them, also they should have full access to the data collected on them. These technologies should help the student not invade their privacy. Also, it should be clear how this data is used and to whom is it provided. The student should be aware of the pros and cons and in case of a data leak, they should be noticed immediately.*

Conclusions

Students express concerns about data security, fearing potential misuse of collected personal information:

- While some support using tools like facial recognition cameras for safety, particularly in dormitories, others stress the importance of privacy and minimizing data collection.
- Suggestions include using unobtrusive monitoring systems and ensuring users can control the extent of shared data.
- Physical safety measures, such as marking bomb shelters on campuses and employing security guards, are preferred over reliance on cameras.
- Students advocate for a fast notification system for threats and emphasize the need for trust, privacy, and community support over invasive technology.
- In conclusion, it can be stated that security (or the lack thereof) is not such a big problem in Estonia, and in particular, the human dimension in ensuring physical security is emphasised, for example, security guards instead of cameras and the important role of fellow university members, who should be more attentive to each other.

References

Aris-Anuar, A. N., Jaini, N., Kamarudin, H., & Nasir, R. A. (2011). Effectiveness evaluation of Safe CityAris-Anuar, A. N., Jaini, N., Kamarudin, H., & Nasir, R. A. (2011). Effectiveness evaluation of Safe City Programme in relation to the tourism industry. Procedia Engineering, 20, 407–414. Programme in relation to the t. Procedia Engineering, 20, 407–414.

Azad, T. B. (2008). Introduction to Security, Editor(s): Tariq Bin Azad, in: Securing Citrix Presentation Server in the Enterprise, Syngress (pp 1-67). https://doi.org/10.1016/B978-1-59749-281-2.00001-9.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. Journal of Advanced Research, 5(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006.

Jeffery, C. R. (1971). Crime Prevention Through Environmental Design. American Behavioral Scientist, 14(4), 598. https://doi.org/10.1177/000276427101400409.

Jennings, W. G., Gover, A. R., & Pudrzynska, D. (2007). Are institutions of higher learning safe? A descriptive study of campus safety issues and self-reported campus victimization among male and female college students. Journal of Criminal Justice Education, 18:2, 191-208. https://doi.org/10.1080/10511250701383327.

Lacinák, M., & Ristvej, J. (2017). Smart city, safety and security. Procedia Engineering, 192, 522–527.

Maier, S. L., & DePrince, B. T. (2020). College students' fear of crime and perception of safety: The influence of personal and university prevention measures. Journal of Criminal Justice education, 31(1), 63-81. https://doi.org/10.1080/10511253.2019.1656757.

Romdhani, I. (2017). Existing Security Scheme for IoT, Editor(s): Shancang Li, Li Da Xu, In: Securing the Internet of Things, Syngress (pp. 119-130). https://doi.org/10.1016/B978-0-12-804458-2.00007-X.

Schafer, J. A., Lee, C., Burruss, G. W., & Giblin, M. J. (2018). College Student Perceptions of Campus Safety Initiatives. Criminal Justice Policy Review, 29(4), 319-340. https://doi.org/10.1177/0887403416631804

Shariati, A., & Guerette, R. T. (2020). The forgotten (practical) side of school safety: What do clery reports say about CPTED and crime on college campuses? Planning Practice & Research, 35(4), 396-417. https://doi.org/10.1080/02697459.2020.1740417.

Van Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472–480. https://doi.org/10.1016/j.giq.2016.

Vitalij, F., Robnik, A., & Alexey, T. (2012). "Safe City"-an Open and Reliable Solution for a Safe and Smart City. Elektrotehniski Vestnik, 79(5), 262.

THANK YOU
FOR YOUR
ATTENTION!!

SISEKAITSEAKADEEMIA