SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 147

SOME ISSUES WITH THE RIGHT TO PRIVACY IN SMART CITIES

Szymon RUBISZ

Silesian University of Technology, Faculty of Organization and Management, Zabrze; szymon.rubisz@polsl.pl, ORCID: 0000-0002-0999-5855

Purpose: discussion on threats to the right to privacy and measures of its legal protection in a smart city.
Design/methodology/approach: analysis of legal provisions and socio-economic context.
Findings: there are significant threats to the right to privacy in a smart city, posed by both private and public entities. There are, however, relevant national and EU regulations that protect the individuals. Those are usually sufficient, but can limit further development of smart cities.
Originality/value: brief analysis of the existing threats to the right to privacy in a smart city, as well as indication of legal protection measures that apply and which, in some cases, may limit the development of a smart city in a long-term. The starting point for an in-depth analysis of future legal changes in national and EU law.

Keywords: smart city, right to privacy, legal protection, threats to personal rights.

Category of the paper: research paper.

1. Introduction

The city has always been an organism under constant development. Over the centuries, the dynamics of this development went through various phases, but the socio-economic changes, resulting from subsequent technical revolutions, required a significant increase in the use of resources and the demand for wider access to further sources of their acquisition. It turned out, that a growing and developing city generates higher and higher costs, hence the concepts were created that assumed the need to save such resources as energy, time or money (Stawasz et al., 2012; Hoek, 2018). Entering the era of advanced information and communication technologies, especially the Internet of Things (IoT)[1], gave potential to optimize their use.

[1] The Internet of Things is an environment, in which the possibilities of the Internet apply to everyday objects that were not previously considered computers. These devices are connected into a network, thanks to which they can generate and use information and exchange it with each other (Theodorou, and Sklavos, 2019, p. 22).

Rapid increase in the number of urban residents (cf. Santen et al., 2010)[2] implies a significant increase in the number of devices connected to the infrastructure. The need to deal with such rapid urbanization, ubiquity of computer systems, as well as the increase in demand for resources have become the impetus for gradual development of intelligent (or smart) cities. Initiatives for their creation have been a goal of many governments around the world.

It should be mentioned that the functioning of smart cities is also a legal issue. Such a city, through its technological tools, interacts with an inhabitant, which means that their rights, especially privacy, confidentiality or freedom of expression, may be threatened (Kitchin, 2014; Losavio et al., 2018). In the 21st century, these are the key policy and legislation challenges according to the OECD (2011). Smart cities are attractive and comfortable to live in, but, at the same time, they are surveillance cities and knowledge about an individual is desirable for both private and public entities. It is, therefore, necessary to discuss the rights to privacy of "city users" and the possibilities for their legal guarantee.

2. The essence of smart cities

There is probably no universally accepted definition of a smart city (Szymańska, 2015, p. 66). The phenomenon still seems to be at a relatively early stage of development and research (Kitchin, 2015, p. 135). It is worth noting, that sometimes the word "smart" is abused by the city, which is just beginning to use intelligent strategies or technologies, and is referred to as smart for promotional reasons (Kowalski, 2015, p. 108). For one researcher, this concept gives new tools for the city management as an aggregate of objects, communication routes, population and relationships between them. Thanks to various types of innovative solutions, city authorities can make better decisions. It is a combination of many different small projects, integrated with each other, which are joint initiatives of the public and private sectors (Abosaq, 2019). Caragliu, Del Bo and Nijkamp (2009, p. 50) say that city may be considered smart when investments in human and social capital, as well as traditional (transport) and modern (ICT) communication infrastructure, have a positive impact on the economic growth and high quality of life, taking into account appropriate management of natural resources through participatory governance. Specific solutions of smart cities, based on various management models, are analyzed in detail by e.g. Patel, Pitroda and Bhavsar (2016). The enterprise sector, in turn, perceives a smart city from the perspective of its business goals – the ability to easily reach the customer with the most accurately addressed offer. A common interpretative approach is to focus pragmatically on the hardware and software aspects of technical infrastructure and its security (e.g. Rawat and Ghafoor, 2019). Barrionuevo, Berrone and Ricart (2012) say that the

[2] The United Nations Population Fund indicates that more than half of the world's population lives in urban areas, with this rate reaching 66% by 2030.

idea of a smart city is largely based on the integration of advanced information technologies, in order to find intelligent solutions and obtain a better quality of life. Cretu (2012) draws attention to the use of intelligent sensors, tools and data sets, the goal of which is to support the improvement of quality of life. Thanks to this, communities living in such cities shall be guaranteed a happy and healthy life (Guan, 2012). There are also attempts to define the concept of smart cities through a multi-dimensional, holistic approach. According to many authors (Giffinger et al., 2007; Cohen, 2011; Lombardi, 2011; Jonek-Kowalska, and Wolniak, 2019), the concept of such a city must be based primarily on such areas as smart people, smart economy, smart environment, smart governance, smart living and smart mobility.

In addition to the above, there is also the point of view of public administration, for which the management of a smart city opens up completely new possibilities. On the one hand, it is a chance for socio-economic progress, lowering operating costs and improving the quality of life of residents. Achieving these goals is obvious, because it brings certain profits to the general public, and this is a determinant of the assessment of administrative activities, not only in organizational, but also in political terms. On the other hand, the opportunity to take advantage of technological benefits of a smart city is the prospect of gaining more knowledge in the area of life, behavior of residents and fulfillment of their needs. Such information can be useful not only to ensure social well-being, but also to control and surveillance for the desired management of the society.

Therefore, having regard to all aspects of understanding a smart city, one of the challenges for implementing such concept is to build a system that will inspire public confidence. It is the privacy and confidentiality of individual data that should be the overall priority in smart cities (cf. van Zoonen, 2016). It is the public administration that is the critical link in guaranteeing and respecting rights (Keta, 2015). However, one should be aware that, in many places around the world, the provisions protecting these values will only be a facade, while intelligent solutions will serve as very effective tools for strengthening and maintaining political power.

3. The right to privacy

Also, the concept of right to privacy does not have a uniform and comprehensive definition. According to Kopff (1982), it is a personal good, which includes everything that, due to the justified separation of the individual from the society, serves to develop physical and mental personality and preserve the achieved social position. For Braciak (2002), privacy is the interest and good of an individual, which can be protected by undertaking various activities, and which is not subject to external control. The exclusive sphere of an individual includes physical space, objects, buildings to which others do not have access. Depending on the socio-cultural system, in which an individual operates, the sphere of privacy is defined differently in terms of

interaction, degree of distance and level of isolation. Having the above in mind, privacy can be defined as a sphere of personal behavior, customs and information that everyone has, of which the scope of openness in public space depends on the will of an individual or a group, to which these values belong. Therefore, the authorized entity has, among others, the right to protect family life, information about their daily activities, most personal attributes, such as sexual orientation or health condition, information about views or religion, about the message and its content addressed to other people and finally the right to separate from others.

In the literature (Safjan, 1999), attention is drawn to the fact that the protection of privacy should be perceived, on the one hand, in connection to the relationship between individuals (horizontal system) and, on the other hand, the relationship between the individual and public authority (vertical system). The proposed division inclines to an assumption that privacy law in smart cities can also be considered in a similar way. First of all, it is possible to point out violations of the individuals' privacy by other entities or enterprises (e.g. breach of contract provisions or its absence, breach of obligations regarding personal data protection or criminal delicts). Secondly, the personal sphere of an individual may be threatened by public authorities, who may want to interfere in it for political purposes.

4. Threats to privacy in a smart city

Smart cities generate huge amounts of data thanks to the extensive and constantly expanding network of devices connected to the system (cell phones, cameras, drones, service machines, personal computers, cloud computing) and sensors (motion, twilight, infrared, RFID). They support various types of services, such as monitoring, control and optimization of energy flow, intelligent transport systems improving urban traffic, parking systems, vehicles communicating with each other and with the city system, remote health monitoring programs, environmental monitoring sensors, information systems for city users and more. Images from futuristic films of the past are becoming a reality.

Certainly, the use of modern services offered by the city gives many entities interesting and attractive opportunities. In the smart city environment, however, there are many threats that affect the privacy of individuals. The goal of the designed or already implemented technical solutions is to serve the population, meet its needs, improve the quality of life or simply provide comfort. Therefore, many of them must, for obvious reasons, specifically interact with people, e.g. via identification, scanning, checking the current location, including time and direction of movement and then process and properly archive this information for possible subsequent use. This type of monitoring can, undoubtedly, cause anxiety among residents, due to the loss of a certain part of their privacy, the persistence of the feeling that they are constantly monitored and controlled. In addition, there is a distrust that each step can be anticipated and can be used

for various purposes, not necessarily beneficial to the person being observed. Doubts grow even more when we realize what these purposes may actually be and who can access the data collected this way.

Since these technologies are ubiquitous in the urban area and are part of an IT network, there is a risk that they will fall into the wrong hands. Examples of violations include directing unsolicited marketing messages thanks to the data collected from mobile device tracking. Such information was collected for advertising purposes by e.g. Renew in London (Miller, 2013). However, one can imagine much more serious threats using captured private data, such as identity theft, impersonation or stalking. It is obvious that, in order to protect against such activity, it is necessary to use effective encryption methods protecting both the data transmission and its storage place. On the other hand, city users should be universally and constantly provided with appropriate education ensuring their safety, above all on the importance of using proper privacy settings in communication devices connected to the Internet. Various suggestions to constantly familiarize and integrate the community with smart city (Berntzen, and Johansson, 2016) seem to be right. In addition, people should know that their data is being collected and should have easy access to clearly formulated rules (cf. Blum-Dumontet, cited in Volpe, 2018). The best would be to get explicit and informed consent, but it is hard to expect everyone to have to accept a kind of "end-user license agreement" before entering the city. Especially if not everyone knows what it is all about, as Thomas et al. (2015) argue.

In addition to the above, the vertical aspect of the protection of the right to privacy should also be taken into account, i.e., in this context, the relationship between an individual and the public authority (it is worth mentioning that the research cited by van Zoonen (2016) shows greater trust of people in the local government managing their data than national authorities). Earlier in the paper, the existence of a kind of temptation to enter the citizen's private life more deeply has been indicated. The technologies referred to above certainly enable significant expansion of the information resource on each user "connected" to a smart city and, consequently, more effective control. Possible problems with privacy are currently associated mainly with countries such as China – the homeland of half the smart cities in the world, where the authorities are particularly enthusiastic about such projects (Keegan, 2020). There are probably legitimate reasons behind it, related to the rapid urbanization and development of this country, but the authoritarian nature of the Chinese political system does not go unnoticed either. The stability and durability of such a system can provide effective oversight of society, which is willing to sacrifice its rights – freedom of speech, assembly, movement and free communication – just for a more comfortable and safe life (cf. Acquisti et al., 2013). It can be assumed that, in democratic systems, such threats are not real. Perhaps this is the correct assumption in developed and established democracies, despite some issues shown by e.g. Wylie (2018). But in countries that are just building their free political systems, authorities may want to, for particular political interests, take advantage of the potential of concepts of cities that, today, are intelligent and, in the future, perhaps may even be omniscient.

5. Legal measures

The right to privacy is guaranteed by the Polish Constitution, providing for the legal protection of private and family life, honor and good name, as well as to decide about one's personal life (art. 47). The act also protects the secret of communication, integrity of the apartment and states the scope of disclosure of information about a person. These subjective rights can be limited in very special cases only. The discussed rights are also indirectly regulated in the Civil Code in art. 23, which, among human personal rights, does not mention the right to privacy directly, but it results from other listed goods, such as dignity, honor, image or the secret of correspondence (Radwański, 2007, p. 168). Pursuant to the provisions of the Code (art. 24), an entity, whose privacy has been violated, is entitled to protection measures in the form of a demand for cessation, unless the violation was unlawful, and to remove the effects of the violation by a statement of appropriate content and in an appropriate form, demanding financial moral satisfaction or payment of an appropriate amount for a specified social purpose, and in case of damage to property – compensation.

The view of Safjan (2002, 5), that today's civilization reduces the influence of an individual on the scope of information about oneself, seems to still be valid. The protection of privacy by civil law measures becomes difficult or impossible. Institutional protection and boundaries set by public law work more effectively. For instance, Polish Penal Code, in art. 190a, provides for imprisonment of up to 3 years, for persistent harassment of another person, to the one who violates someone's privacy. The same punishment shall apply to anyone who uses someone else's image or other personal data to cause damage to its owner. Other crimes against privacy can be identified in art. 212-217 and they concern, among others, defamation, insults or violation of physical integrity, as well as in art. 267 §1 sanctioning the unlawful acquisition or disclosure of information constituting a private secret.

The right to privacy is often associated with the law on the protection of personal data. In this respect, the EU Regulation, the so-called GDPR, applies in Poland since 2018. The framework of this study does not allow a detailed analysis of the Regulation, but several examples of provisions to protect the individual can be identified. These include the possibility of "pseudonymization" of the data (art. 4, that is, such processing of data that it can no longer be attributed to a specific person, without using additional information), the right to be forgotten (deletion of data, art. 17), the right to object to the processing of personal data (art. 21), profiling restrictions (art. 22), numerous obligations of data processors with regard to keeping detailed documentation and records regarding processed data, the need to obtain valid and verifiable consents to data processing and, finally, to assess the impact of data protection in case of sensitive activities, such as large-scale profiling or the use of specific categories of data (such as health data). Anyone who suffers material or non-material damage as a result of a breach of the Regulation has the right to receive financial compensation from the data processor or

administrator (art. 82). EU has decided to harmonize the protection of data and the provisions should effectively protect the subjects' rights. They simultaneously seem to limit the development of smart cities in some areas (cf. Losavio et al., 2018), especially in those countries, where data protection was low. However, where its level was high enough, adaptation to the GDPR should not be a problem (Vojković, 2018).

This short and non-exhaustive review of applicable regulations allows us to conclude that the entity has strong legal means to protect its privacy in a smart city. One can have some doubts as to their effectiveness in the relationship between the individual and public authority in the limitation of the principles of a democratic rule of law observed in many places around the world. In each case, however, the resolution of any conflict will remain with national- and ultimately supranational courts.

6. Conclusion

The planning, design and implementation of a smart city by public administration must definitely take into account the right to privacy of an individual. There is a number of identified threats to these rights, which may come from both private and public entities. People are ready to give away some of their privacy if, in return, they receive attractive services that improve their lives; only some care about being watched. They must, however, be aware that any device connected to the smart city can be a source of useful information – about users' habits, locations, activities, also these potentially illegal, immoral or politically inappropriate.

Adequate technical security, as well as providing detailed and easy-to-learn information for the city user about the conditions for collecting and processing data and the possibility of asserting their rights under applicable regulations, are basic tasks to be performed by the authorities, local and national. They must be aware that a smart city is not only a managerial or technological issue, but also legal and political. The needs of the state and of modernity, with respect to individual rights, are the main challenge for the implementation of smart cities in the frames of applicable law.

The enormity and completeness of the collected data are, as said above, a rich source of information about the individual, so the conflict between the authorities and the citizen seems possible. Its scale depends on internal regulations. Of course, there are relevant and sufficient constitutional, civil, administrative and penal provisions, as well as EU regulations, that support protection of the right to privacy. Sometimes it is necessary to mention that they can even limit too far-reaching impulses in the development of smart cities (like GDPR). However, they won't be effective if public authorities take advantage of the opportunity to manage society more effectively at the expense of democratic principles.

References

1. Abosaq, N.H. (2019). Impact of Privacy Issues on Smart City Services in a Model Smart City. *International Journal of Advanced Computer Science and Applications, 10(1),* pp. 1-9.
2. Acquisti, A., John, L.K., Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42(2),* pp. 249-274.
3. Barrionuevo, J.M., Berrone, P., Ricart, J.E. (2012). Smart Cities, Sustainable Progress, *IESE Insight, 14,* pp. 50-57.
4. Berntzen, L., Johansson, M.R. (2016). The role of citizen participation in municipal Smart City projects: Lessons learned from Norway. In: *Smarter as the new urban agenda* (pp. 299-314). Cham: Springer.
5. Braciak, J. (2002). *Prawo do prywatności.* In: B. Banaszak, A. Preisner (Eds.), *Prawa i wolności obywatelskie w Konstytucji RP.* Warszawa: C.H. Beck.
6. Caragliu, A., Del Bo, C., and Nijkamp, P. (2009). Smart cities in Europe. *Journal of Urban Technology, 18(0048),* pp. 45-59.
7. Cohen, B. (2011). The Top 10 Smart Cities On The Planet. *Fast Company.* Retrieved from https://www.fastcompany.com/90186037/the-top-10-smart-cities-on-the-planet, 20.04.2020.
8. Cretu, G.L. (2012). Smart Cities Design Using Event-Driven Paradigm and Semantic Web. *Informatica Economica, 16(4),* pp. 57-67.
9. Giffinger, R., et al. (2007). *Smart cities. Ranking of European medium-sized cities.* Vienna University of Technology.
10. Guan, L. (2012). Smart Steps to a Battery City. *Government News, 32(2),* pp. 24-27.
11. Hoek, M. (2018). *The Trillion Dollar Shift.* London: Routledge.
12. Jonek-Kowalska, I., Wolniak, R. (2019). *Holistyczne podejście do rozwoju inteligentnych miast*. In: I. Jonek-Kowalska (Ed.), *Wyzwania i uwarunkowania zarządzania inteligentnymi miastami* (pp. 23-40). Zabrze: Wydawnictwo Politechniki Śląskiej.
13. Keegan, M. (2020). In China, Smart Cities or Surveillance Cities? *U.S. News*. Retrieved from https://www.usnews.com/news/cities/articles/2020-01-31/are-chinas-smart-cities-really-surveillance-cities, 20.04.2020.
14. Keta, M. (2015). Smart city, smart administration and sustainable development. *Romanian Economic and Business Review, 10(3)*, pp. 43-56.
15. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79(1),* pp. 1-14.
16. Kitchin, R. (2015). Making Sense of Smart Cities: Addressing Present Shortcomings. *Cambridge Journal of Regions, Economy and Society, 8(1),* pp. 131-136.

17. Kopff, A. (1982). Ochrona sfery życia prywatnego w świetle doktryny i orzecznictwa. *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace prawnicze, 100.* Kraków: PWN.
18. Kowalski, Ł. (2015). *Inteligentne miasta – przegląd rozwiązań*. In: P. Trzepacz, J. Więcław-Michniewska, A. Brzosko-Sermak, A. Kołoś (Eds.), *Miasto w badaniach geografów* (pp. 105-121). Kraków: IGiGP UJ.
19. Litwiński, P. (2020). Aplikacja ProteGO. Należy nazwać ten projekt po imieniu: To profilowanie obywateli. *Gazeta Prawna*. Retrieved from https://prawo.gazetaprawna .pl/artykuly/1467429,aplikacja-protego-koronawirus-profilowanie-obywateli.html, 20.04.2020.
20. Lombardi, P. (2011). New challenges in the evaluation of smart cities. *Network Industries Quarterly, 13(3),* pp. 8-10.
21. Losavio, M.M., Chow, K.P., Koltas, A., James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy, 1(3)*. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.23.
22. Miller, J. (2013). City of London calls halt to smartphone tracking bins. *BBC News*, Retrieved from https://www.bbc.com/news/technology-23665490 20.04.2020.
23. OECD (2011). *Digital identity management. Enabling innovation and trust in the internet economy*. Retrieved from http://www.oecd.org/internet/ieconomy/49338380.pdf.
24. Patel, M.B., Pitroda, J., Bhavsar, J.J. (2016). Success Factor for Smart Infrastructure Development through Lean Management: A Review, *Conference: 21st ISTE State Annual Faculty Convention and National Conference on "Emerging Trends in Engineering" at Tolani Foundation Gandhidham Polytechnic.* Adipur.
25. Radwański, Z. (2007). *Prawo cywilne – część ogólna.* Warszawa: C.H. Beck.
26. Rawat, D.B., Ghafoor, K.Z. (2019). *Smart cities cybersecurity and privacy.* Elsevier.
27. Safjan M. (2002). Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym. *Państwo i Prawo, 6,* pp. 3-12.
28. Safjan, M. (1999). *Ochrona danych osobowych – granice autonomii informacji*. In: M. Wyrzykowski (Ed.), *Ochrona danych osobowych.* Warszawa: Instytut Spraw Publicznych.
29. Santan, R. van, Khoe, D., Vermeer, B. (2010). *2030 Technology that will change the world.* New York: Oxford University Press.
30. Stawasz, D., Sikora-Fernandez, D., Turała, M. (2012). Koncepcja Smart City jako wyznacznik podejmowania decyzji związanych z funkcjonowaniem i rozwojem miasta. *Zeszyty Naukowe Uniwersytetu Szczecińskiego, 721, Studia Informatica, 29,* pp. 97-109.
31. Theodorou, S., Sklavos, N. (2019). *Blockchain-Based Security and Privacy in Smart Cities*. In: D.B. Rawat, K.Z. Ghafoor (Eds.), *Smart Cities Cybersecurity and Privacy* (pp. 21-37). Elsevier.

32. Thomas, V., Mullagh, L., Wang, D., Dunn, N. (2015), *Where's Wally? In search of citizen perspectives on the smart city*, 8th conference of the international forum on urbanism (IFoU). Multidisciplinary Digital Publishing Institute, pp. 1-8.
33. Vojkovic, G. (2018), Will the GDPR slow down development of Smart Cities? In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1295-1297. IEEE.
34. Volpe, A.M. (2018), *Are smart cities ready for Europe's new privacy measures?* Retrieved from https://cordis.europa.eu/article/id/124305-are-smart-cities-ready-for-europes-new-privacy-measures
35. Wylie, B. (2018), *Searching for the Smart City's Democratic Future*, Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/articles/searching-smart-citys-democratic-future
36. Zoonen, L. van, (2016), *Privacy concerns in smart cities*, Government Information Qarterly 33(3), pp. 472-480.