Секція 3

Інформаційні технології

Mechanisms of public management in the personal data protection in smart cities

Dmytro Khlaponin

State university of telecommunications
Solomyanska st. 7, Kyiv, Ukraine, 03110
kmld.85@gmail.com

INTRODUCTION

More than ten years ago in the world has emerged the concept “smart city” and till today smart cities have developed in many countries of the world.

A smart city is a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business [1].

Any smart city, in turn, consists of a huge amount of cyber physical systems (CPSs).

Cyber physical systems are smart systems that include engineered interacting networks of physical and computational components [2].

The essential requirements to functioning of these systems are safety, security, reliability, resilience, confidentiality. Automated decision-making, including profiling in the personal data processing constitutes a significant part of cyber physical systems as components of smart cities.

As the personal data is processed automatically, computations are performed in the “cloud” in the network of distant servers, there is a risk of various cyber threats and real cyber attacks on certain cyber physical system (as part of a smart city) which may cause a damage or losses to the personal data subject as a result of unlawful destruction, use, alteration or disclosure of the personal data.

The Ukrainian legislation does not contain the concept “smart city”. The unsolved problem in the Ukrainian legislation is the recognition of the personal data subject as a central element of any cyber physical system (as part of a smart city) and the necessity of ensuring balance between the fundamental rights and freedoms of the personal data subject and the rights of the data possessors, data processors, data protection officials, the authority of the Commissioner of the Verkhovna Rada of Ukraine on human rights who gain access to the personal data by means of personal data subject consent.

The comparative analysis of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (Regulation) [5] with the Ukrainian Law [4] which refers to various elements of the processing of personal data in different processing systems, to the rights and obligations of the data controller, the data processor, the supervisory authority with regard to ensuring lawful, secure, confidential processing of personal data is made.

THE PURPOSE OF THE RESEARCH

The purpose of the research is to analyze the personal data protection in accordance with the Regulation [5] in comparison with the Law “On the personal data protection” [4] aimed at the revealing of the progressive provisions of the Regulation which refer to the various elements of the processing of personal data in different processing systems (including CPSs as components of smart cities), to the rights and obligations of the data controller, the data processor, the supervisory authority with regard to ensuring lawful, secure, confidential processing of personal data.

MAIN BODY

Smart cities employ a combination of data collection, processing, and disseminating technologies in conjunction with networking and computing technologies and data security and privacy measures encouraging the application of innovation to promote the overall quality of life for its citizens and covering dimensions that include: utilities, health, transportation, entertainment and government services [3].

CPSs as components of a smart city integrate computing, communication, data storage with real world's objects and physical processes. All the above-mentioned processes must occur in real-time, in a safe, secure and efficient manner.

According to the Article 2 of the Law [4] personal data is the information or a set of information about an individual that is identified or can be specifically identified. According to the Article 4 of the Regulation [5] "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In accordance with Article 4 of the Regulation 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [5].

The Ukrainian law [4] does not contain the concept "pseudonymisation", however this concept is extremely important in personal data protection in different areas as well as in the operation of CPSs as components of smart cities. Therefore, the concept "personal data depersonalization" should be substituted in the Ukrainian law with the concept "pseudonymisation" with the abovementioned definition.

In accordance with the Article 4 of the Regulation [5] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

It can be concluded that "profiling" can be performed in CPSs as components of smart cities in such areas as healthcare, energy (smart grid), traffic management etc. The Ukrainian law does not contain the concept "profiling". This concept should be introduced into the law with the abovementioned definition.

Article 5 of the Regulation [5] defines certain Principles relating to processing of personal data. It is indicated that personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'); (d) accurate and, where necessary, kept up to date; ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

All these principles are crucial to the processing of personal data in any kind of legal relationship between the natural and legal persons, public authority and other subjects as well as in the operation of CPSs as components of smart cities. However the principle "integrity and confidentiality" is one of the most important principles and is ensured by the appropriate technical characteristics in the design of CPS as part of a smart city. If this principle is not ensured in the design of CPS this system will be subject to cyber attacks of different levels of complexity with the subsequent damage to the secure, reliable, resilient functioning of CPS (as part of a smart city) and confidential processing of the personal data will not be guaranteed.

In conformity with Paragraph 1 of the Article 22 of the Regulation [5] the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The similar provision is layed down in the Article 8 of the Law [4] which emphasizes that the personal data subject shall have the right to the protection from the automated decision which produces legal effects concerning him or her.

For instance, in CPS as part of a smart city personal data is automatically processed in order to fulfil the functions of CPS in certain areas of deployment. Automated processing and computation are performed in the cloud (with many distant servers) and are inevitable for the appropriate functioning of CPS as part of a smart city. However, these operations in the cloud may constitute a risk of personal data breach and to avoid such consequences an appropriate technical measures should be taken by the CPS operator in order to ensure security and confidentiality of the personal data.

CONCLUSIONS

According to the definition of the concept "controller" in the Regulation [5] it has the same meaning as the concept "possessor" in the Ukrainian Law [4].

Therefore the controller as well as the possessor shall ensure the appropriate safeguards to the personal data protection, which may include encryption or pseudonymisation. The essential requirement to the security and confidentiality of the personal data in any kind of processing systems (including CPS as part of a smart city) is that different types of personal data relating to a relevant natural person shall be kept separately in order to avoid easy establishment of that person and an obligation of professional secrecy shall be strictly observed by the controller as well as the possessor.

Keywords: Cyber physical system, smart city, personal data protection, encryption, pseudonymisation.

REFERENCES

1. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.
2. **Framework** for Cyber-Physical Systems Release 1.0 May 2016 CPS Public Working Group. Retrieved from www.nist.gov.
3. **Gharaibeh A.; Salahuddin M.A., Hussini S.J., Khreishah A., Khalil I., Guizani M., Al-Fuqaha A., 2017**. Smart Cities: A Sur-ey on Data Management, Security, and Enabling Technologies. IEEE Communications Surveys & Tutorials. 19(4), 2456–2501. doi:10.1109/COMST.2017.2736886.
4. **On the personal** data protection: Law of Ukraine 1st June **2010**. № 2297-VI Retrieved from http://zakon3.rada.gov.ua/laws/show/2297-17.
5. **The Regulation** (EU) 2016/679 of the European Parliament and of the Council of 27 April **2016** 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. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.