ETHICAL ASPECTS AND PERSONAL DATA PROTECTION IN THE EXECUTION OF HOME PRISON PENALTY[1]

Lucas Michalov
Doctor of Law, Professor, Faculty of Law, University of Pavel Joseph Shafarik in Kosice, Slovakia
lab.kkonkpr@msal.ru

Diana Treshchakova
Doctor of Law, Professor, Faculty of Law, University of Pavel Joseph Shafarik in Kosice, Slovakia
lab.kkonkpr@msal.ru

Abstract. *The home prison penalty is currently a part of the sanction system in the Slovak Republic and serves as a manifestation of so-called restorative justice. Restorative justice is represented by alternative sentences that are distinguished from real imprisonment for minor offences. Alternative penalties may include penalties that do not involve the deprivation of liberty associated with the isolation of a convicted person. The advantage of alternative sentences is that the offender is spared the destructive effects of imprisonment. The offender is not exposed to the negative aspects of this punishment and remains integrated into the society, being able to continue to maintain social, family and working relations, which can significantly improve the protection from the offender.*

At present, there are many unresolved issues regarding the execution of the punishment of home prison penalty, especially its execution through electronic monitoring, including the protection of personal data obtained through electronic monitoring equipment. Thus, the purpose of this article is to focus on these issues and present the authors' views.

Keywords: *home prison penalty, electronic monitoring, type of punishments, EU, elaboration*

Development of Home prison penalty

Home prison penalty has gone through its gradual development. This institute has been used in past especially in the private sector. It was used to people who were strong or influential to be placed in a real prison. For example, hereditary rulers, prominent political figures, religious leaders whose imprisonment could cause rebellion. The first mention of the institution of home prison is the detention of the Apostle Paul. Many former presidents have been sentenced to home prison for crimes against their countries, for example Pol Pot (Cambodia), Rafael Videla (Argentina), Habib Bourgiba (Tunisia), Aung San Suu Kyi (Burma). Former dictator Augusto Pinochet was placed

[1] This scientific paper came with support and is the output of a research project of the Agency for the Support of Research and Development in Slovak republic in the framework of the project: Privatization of Criminal Law — substantive, procedural, criminological and organizational - technical aspects; no. APVV-16-0362; Tento článok vznikol s podporou a je výstupom riešenia výskumného projektu Agentúry na podporu výskumu a vývoja v rámci projektu: Privatizácia trestného práva — hmotnoprávne, procesnoprávne, kriminologické a organizačno-technické aspekty; č. APVV-16-0362 a APVV-14-0598 Elektronizácia v podnikaní s akcentom na právne a technické aspekty — "Electronization in business undertaking focusing on legal and technical aspects".

in home prison upon order. A former leader had been placed in home prison for the last 16 years of his life. Former Prime Minister of the Soviet Union Nikita Khrushchev was placed in home prison for seven years before his death after being overthrown in 1964.[2]

Even in the historical development of the home prison, it was clear that without technical control, this sentence will be ineffective. In the mid-1960s, the first electronic monitoring device was developed by Harvard psychologist Dr. Ralph Schwitzgebel, who worked on the Science Committee in Psychological Experiments at Harvard University. In 1964 he developed one kilogram weighing radio telemetry device, which consisted of a battery and a transmitter and transmitted signals that could be traced to a distance of 400 meters and determine the whereabouts of the wearer. Dr. Schwitzgebel hypothesized that his invention could provide a more humane and cheaper alternative to detention for many people involved in the justice process. This device was patented in 1969. However, this device came into practice only in 1977 when Judge Jack Love from Albuquerque, New Mexico, inspired by an episode from the cartoon series Spiderman, discovered the possible use of electronic monitoring. Judge Love convinced Michael Goss, an electronics specialist, to manufacture and construct an electronic control device. In 1983, Judge Love sentenced the perpetrator to a home prison with electronic monitoring for the first time. Subsequently, other states began to use this institute. Electronic surveillance systems grew at the fastest rate in the United States of America, and by 1988 they were already in place in 32 countries, with a total of 2 300 offenders monitored electronically.

However, the home prison is not a completely new institute even in the Slovak republic. It was already regulated in the Criminal Code no.117/1852 Coll. Home prison was essentially an alternative to first-instance prison and could be imposed if the offender had no criminal records. He had to undertake not to leave the house under any excuse, otherwise he had to execute the remainder of his sentence in prison because of a breach of the obligation. Sometimes the oath was necessary, sometimes the guard was present.

Present legislation

Home prison penalty was re-enacted in the Slovak legislation upon re-codification of Criminal Code with the effect from January 01, 2006. We can recognize two types of home prison, “Front-end” type and “Back-end type”. “Front-end“ type of home prison means that the criminal could spend all time of penalty in home prison. “Back-end” type means that criminal firstly go to a real prison and if the behaviour is acceptable, criminal can spend final stage of penalty in home prison. “Back-end” type has been regulated in Slovak Criminal Code since 2016.

Home prison is considered as an alternative sanction to imprisonment for less serious criminal acts, to which the home prison penalty can be imposed to the criminal in duration up to four years. Criminal Code regulates that the court may impose a home prison penalty for a crime where the upper limit of penalty rate of imprisonment is max-

[2] RAJNIČ, M.: Trest domáceho väzenia v systéme trestov. Justičná revue, 61, 2009, č. 6-7

imum ten years. Criminal Code regulates the terms of home prison penalty awarding which have to be fulfilled cumulatively.

The home prison penalty may be imposed if:

— in view of the nature of the crime committed by offender imprisonment is not necessary due to criminal personality circumstances of the crime,
— the offender has given a written statement to reside in the dwelling at the specified address at a specified time and to provide the necessary assistance in carrying out the inspection and control,
— the conditions for carrying out control by technical means are fulfilled.

By imposing the home prison penalty, the court must take in account evaluation criteria related to the nature and importance of the offence committed, and also the offender. In case of offences, the court of justice makes assessment of criminal act commitment method, its consequences, circumstances of the act commitment, the blame rate and offender´s motive. The court should consider the nature of criminal activity, personal and family conditions future criminal´s prognosis and re-socialization possibilities. Another condition representing the essence of home prison penalty corresponds to written statement of the offender declaring that criminal will stay in the determined address and provide required cooperation during control.[3]

Sentenced criminal is obliged to stay in his residence including adjacent premises, to live a respectful life and to withstand control by technical means during period of home prison penalty execution during the time period determined by the court. The court deciding on home prison penalty should specify exact place of home prison penalty in the verdict where the sentenced person shall stay. The judge should also specify exact time in the verdict when the sentenced person shall stay in the residence. Judicial praxis demonstrated that obligation to stay in the residence applies to the weekly working days and out of the working time within approx. 7:30 PM — 06:00 AM. To ensure that the sentenced person runs a proper working and family life during the home prison penalty execution.

For the duration of the home prison penalty, the person may leave his or her dwelling only with the prior consent of the probation and mediation officer, and only on imperative grounds and for the necessary time. This time counts towards the sentence.

If the sentenced person fails to fulfil obligations imposed by the court of justice, and restrictions resulting from the home prison penalty, the court shall change the home prison penalty or a part of it to imprisonment. Criminal Code stipulates the way of changing the home prison penalty to unconditional imprisonment in proportion 1:1, following prior hearing of the sentenced person. It means that one pending day of the home prison penalty shall correspond to one day of imprisonment and the court of justice shall decide on the way of such imprisonment.

[3] TÓTHOVÁ, V., FERENČÍKOVÁ, S. (2019). INNOVATION IN CRIMINAL POLICY OF IMPOSING ALTERANTIVE SANCTIONS IN SLOVAK REPUBLIC. In P. Hájek, & O. Vít (Ed.), CBU International Conference Proceedings. 7, pp. 661-670. Prague: CBU Research Institute. Doi:https://doi.org/10.12955/cbup.v7.1435

Control by Electronic monitoring

Essential term of home prison penalty imposing is that the conditions for carrying out control by technical means are fulfilled. Control of home prison penalty execution by technical means can be undoubtedly considered innovation in relation to control of sanction execution in general.

Electronic monitoring is Slovak republic was enacted in the legislation upon Act No. 78/2015 Coll. on Control of Certain Decisions Execution by Technical Means as amended. The Act became effective on January 01, 2016 and the Electronic System of Persons Monitoring was established in Slovakia on the same date. Act No. 78/2015 Coll. Regulates technical means, their terms of use and the course of control.

Electronic monitoring represents the system of monitoring the observance of certain bans, restrictions and orders, as well as sanctions and certain protection measures as the forms of penal law sanctions. Pursuant to regulation in effect, we distinguish six types of monitoring where different types of technical means are used in each type of monitoring.

Technical means operating cost is borne by the state and partly by the monitored person. Amount of its share is determined in the executive command. Technical means are the state property connected to a so-called central monitoring system. It is this that allows for the check of the detainment regime observance through signals transmitted by technical means, and the record of security and operating incidents.[4]

Effective control of sentences without deprivation of liberty can be ensured through technical means and electronic monitoring. The project of the electronic system for monitoring accused and sentenced persons (ESMO), co-funded by the European Union from the European Regional Development Fund through the Operational Program Informatization of the Company was launched by the Ministry of Justice of the Slovak republic in 2013.

The Act on the control of the enforcement of certain decisions by technical means distinguishes more types of technical means. For home prison penalty execution, it is necessary to use

(1) personal identification device,

(2) a device for checking presence at the place of sentence,

(3) the Probationary and Mediation officer's device

The basic element of the electronic monitoring and technical means is the personal identification device — currently in the form of a bracelet, which is set on the body of the monitored person, usually on his / her ankle. The monitored person is obliged to tolerate the attachment of this device to his / her body throughout the duration of the enforcement of the decision by technical means. Any attempts to interfere with this device or to damage or destroy it are evaluated as security incidents. This general device is used in the execution of a home prison penalty, by the imposition of various appropriate limitations and obligations.

[4] KLÁTIK, J.. Uplatňovanie restoratívnej justície a elektronického monitoringu na Slovensku a vo vybraných štátoch Európskej únie. I. KOŠICKÉ DNI TRESTNÉHO PRÁVA — Perspektívy vývoja európskeho trestného práva. Košice, 2018. Univerzita Pavla Jozefa Šafárika v Košiciach

A device for checking presence at the place of sentence used in home prison penalty is located in the dwelling (house, apartment, residence) of the monitored person and on the basis of communication with the personal identification device, it is possible to check the presence of the monitored person at a specified time in the specific place. At present, this device is in a form of home monitoring station. This device communicates with a personal identification device whose radio frequency signal receives and evaluates the presence and the absence of the monitored person at a specified place and at a specified time, in accordance with a court decision. In the event of a violation of the conditions, this device will signal this fact to the Operations Center, which will pass this information to the relevant Probationary and Mediation Officer.

The probationary and mediation officer's device is used by a probationary and a mediation officer. This technical device enables a probationary and a mediation officer to carry out a control of prohibition, limitation, or obligation "on-site" (on place) by identifying the presence of a personal identification device within a range of approximately 300 m in its geographic conditions, and thereby detect the presence of people who have this device connected to the body. In a particular case, for example, it will be possible to verify whether the controlled person is at a specified time in the designated place or, on the other hand, is not in the specified place at a specified time.

Ethical aspects of electronic monitoring

Electronic monitoring device also includes automated data processing of sentenced criminals. It is an innovative way of the execution of a punishment through an electronic device, which can also be classified under the use of artificial intelligence.

Nowadays, especially at the age of the 4th Industrial Revolution, artificial intelligence is being introduced in every area of our functioning, including the execution of punishments of sentenced criminals. It is precisely because of the introduction of artificial intelligence into the execution of punishments is necessary to examine the nature of artificial intelligence and its legal and ethical aspects.

It can be stated that artificial intelligence is a scientific discipline that deals with the development of algorithms and machines that show signs of intelligent behaviour. Given the unstoppable development of artificial intelligence, it is necessary to solve its question in a normative way and to take precautions to prevent its abuse.

In June 2018, the European Commission set up an expert group — AI HLEG, composed of public, industry and academic figures. This group prepared a document supporting the European Commission's strategy on artificial intelligence and robotics. However, as they point out, the document is the result of the work of the group and cannot be regarded as an official position of the Commission. The document focuses mainly on ethical values and resilience, from the technical side as well as socially. The development and integration of artificial intelligence into life should be based on four ethical principles, based on the Charter of Fundamental Rights of the European Union, namely:

1. Prevention of harm — the principle is based on an article on the inviolability of a person, both in physical and mental form, specifically from the perspective of medicine and biology, for example prohibition of the reproductive cloning of the human being, the full text of which can be found in Article 3 of the Charter.

2. Respect for human autonomy — the artificial intelligence system cannot weaken or otherwise adversely affect it. The human has the ability to oversee the system and intervene in the process.

3. Justice — takes different forms, but the development of the system should be fair in terms of two dimensions. The substantive dimension includes an equal distribution of costs and benefits as well as ensuring that a person is not exposed to discrimination or bias. The procedural dimension includes the possibility to reject the decisions of the artificial intelligence system and people and insist on remedy. For this purpose it must be possible to identify the body responsible for the decision and the decision-making processes should be explained.

4. Clarity — to ensure that the artificial intelligence system is always transparent so that procedures can be identified and openly communicated about the purposes of the system.

These ethical principles have resulted in ethical requirements that must be followed when implementing the so-called. trustworthy artificial intelligence.[5]

On 07.12.2018, the European Commission presented to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions a Communication on a "*Coordinated Artificial Intelligence Plan*" accompanying the Coordinated Plan for the Development and Use of Artificial Intelligence Developed by Member States (as part of the European Industry and Artificial Intelligence Group), Norway, Switzerland and the Commission[6]

The coordinated plan covers four key areas, namely:

a) increasing investments;
b) declassifying and cumulating more data (which is a 'raw material' for artificial intelligence)
c) support for talent
d) ensuring confidence

They identified priority areas of public interest, such as health care, transport and mobility, security, security and energy, as well as important economic sectors such as manufacturing and financial services.

The questions that we need to ask about the deployment of artificial intelligence therefore have not only a technical but also an ethical dimension. The first of the ethical problems is the transparency and clarity of artificial intelligence decisions, what is related to the problem of traceability of possible errors in the automatic decision making of the machine. Programs that predict criminal behaviour are examples of how poorly transparent the decision based on artificial intelligence is and how it can have a serious impact on people. These may be, for example, algorithms that estimate which persons are most likely to be involved in illegal activity or assess the likelihood of recurrence of convicted criminals. Mentioned tools include a system that calculates the degree of danger to convicts for society. Some artificial intelligence decisions have been shown to be discriminatory and racially oriented in this case.

---

[5] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[6] *Coordinated Artificial Intelligence Plan* available on https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/sk/pdf

One reason could be that artificial intelligence acquires its capabilities by observing historical data.[7]

The Recommendation CM / Rec (2014) 4 of the Committee of Ministers of the Member States on electronic monitoring can also be applied to address ethical issues related to electronic monitoring of convicts. This Recommendation addresses ethical issues in Part Five of the Appendix (Part V), which contains Articles 26 to 28. According to Article 26, age, disability and other relevant specific conditions or personal circumstances of each suspect or offender shall be taken into account in deciding whether and under what modalities of execution electronic monitoring may be imposed.

Under Article 27, under no circumstances may electronic monitoring equipment be used to cause intentional physical or mental harm or suffering to a suspect or an offender.

According to Article 28, rules regarding the use of electronic monitoring shall be periodically reviewed in order to take into account the technological developments in the area so as to avoid undue intrusiveness into the private and family life of suspects, offenders and other persons affected.[8]

Personal data protection and electronic monitoring

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Pursuant to par. 26 of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal

[7] https://vedanadosah.cvtisr.sk/etika-a-umela-inteligencia

[8] The Recommendation CM / Rec (2014) 4 of the Committee of Ministers of the Member States on electronic monitoring

data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. These principles must also be applied to electronic monitoring of sentenced criminals.

Electronic monitoring of sentenced criminals is based on the exploitation of artificial intelligence and automated processing of this data. The data obtained from this automated processing are personal data of the sentenced persons and other persons with whom they come into contact. It also can be a sensitive privacy information. This is also related to the issue of big data and profiling of data subjects. A Big Data and profiling of data subject can be understood as processing of a large amounts of information (not just personal data) of different individuals, which primarily consists of analysing and combining this data through a complex of algorithms to find precisely defined relationships, resulting in profiles applicable to groups individuals, which are divided into predefined categories of individuals or groups of individuals according to the anticipated future behaviour of these groups.[9]

The profiling of data subjects is defined also in the General Regulation of the European Parliament and of the Council (EU) from 27th of 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 (General Data Protection Regulation) (hereinafter as "GDPR"). Pursuant to Art. 4 par. 4 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*"

Pursuing to GDPR the data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects without any human intervention. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions (for example racial, ethnic, or religious information). The exception is the public interest and consent of the data subject.

Pursuant to Art. 66 par. 3 Act no. 18/1918 on the protection of personal data is prohibited profiling that leads to discrimination against persons on the basis of specific

[9] HUČKOVÁ, R. — SOKOL, P., RÓZENFELDOVÁ, L.: 4th industrial revolution and challenges for european law (with special attention to the concept of digital single market). In: EU and comparative law issues and challenges series : Eu law in context — adjustment to membership and challenges of the enlargement : International Scientific Conference. — Osijek : Sveučilište Josipa Jurja Strossmayera u Osijeku, 2018., S. 201-215, available on https://hrcak.srce.hr/ojs/index.php/eclic/issue/view/313/Vol2.

categories of personal data. Profiling that is not lawful is also prohibited. Although profiling is otherwise legal and can be helpful in many cases, the data subject has the right to take exception at any time. On the basis of the data subject's exception to profiling, which is otherwise authorized and lawful under the GDPR, processing must be terminated unless the operator can demonstrate convincing legitimate reasons for processing that take precedence over the interests, rights and freedoms of the data subject.

As mentioned above, the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data is modified by specified act of EU that deals also with automated processing of personal data. This is subject to Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter as "direction") in connection with GDPR.

As Mihók points out, it is therefore an important question to examine the possibility of using artificial intelligence in electronic monitoring in criminal justice if pursuant to Art. 22 par. 1 GDPR electronically monitored offenders shall have the right not to be subject to a decision based solely on automated processing, including profiling.[10]

For an adoption of a decision based on an automated processing of data obtained through electronic monitoring, which is also according to GDPR and the Directive, the decision must be adopted by a person or a body designated for this purpose after verification and evaluation of the information received. Of course, it will be appropriate that the assessment of the sentenced person does not take into account data that discriminates the sentenced criminal, as well as data and information not related to him, but concerning, for example, family members.

Pursuant to par. 37, 38 of the directive the data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions

[10] ŽUĽOVÁ, J. 2018. Profilovanie a automatizované rozhodovanie (nielen) v pracovnoprávnych vzťahoch. In ŠVEC, M. — BULLA, M. (eds). *Práca 4.0, digitálna spoločnosť a pracovné právo [online]. [citované 06.09.2019].* Bratislava: Friedrich Ebert Stiftung (zastúpenie v SR), s. 49 - 60. ISBN 978-80-89149-58-2. Dostupné na: http://www.fes.sk/fileadmin/user_upload/aktuality/2018/Praca_4.0.pdf. In. MIHÓK, P.: Vybrané právne a etické aspekty umelej inteligencie pri elektronickom monitoringu obvinených a odsúdených osôb. In. SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.): *Právo, obchod, ekonomika IX.* Košice: Univerzita P. J. Šafárika v Košiciach, 2019

laid down in Articles 21 and 52 of the Charter. Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin. Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data.

It is also important to solve the question how to deal with data obtained from electronic monitoring. Two groups of data and information can be distinguished here. One is the data that is needed to adopt a decision. It cannot be based on special categories of personal data. The second group of data obtained are those which are not necessary to take a decision or do not concern the person concerned. These may be, for example, family members or other persons with whom the sentenced criminal comes into contact. These data must not be used and must be discarded.

The protection of personal data in the electronic monitoring of sentenced criminals should not be done without institutes such as anonymisation and pseudonymisation, which should be used in electronic monitoring.

Personal data protection Act No 18/2018 Coll. in Slovakia following the model of GDPR introduces and define the legal term "pseudonymisation". Pursuant to a par. 5 let. h) "*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.*"

Essentially, the GPDR introduces a completely new concept in European data protection law — pseudonymisation — for a process that handles data nor anonymous but nor directly identifying. As Veselý states, there are many discussions on the extent to which pseudonymised data can be re-identified. Re-identification is crucial as it strongly determines whether or not a particular processing operation of personal data will comply with the provisions of the GDPR Regulation or not, which focuses on the risk that data will identify identifiable persons.

The fundamental difference between pseudonymised data directly regulated in GDPR and anonymous data that is not regulated in the Regulation is not whether personal data can be retrieved with reasonable effort in terms of time, costs and labour. Thus, pseudonymisation involves the removal or disguise of direct identifiers and, in certain cases, indirect identifiers, which could together reveal the identity of a particular person.[11]

[11] VESELÝ, P.: Pseudonymizácia a anonymizácia osobných údajov ako požiadavka GDPR. Available on https://www.zoou.sk/33/pseudonymizacia-a-anonymizacia-osobnych-udajov-ako-poziadavka-gdpr-uniqueidmRRWSbk196FPkyDafLfWAJWc7pG-Xzb6XqJG803ba64/

It is important that in order to protect personal data these are pseudonymised and that even in breaching of their security and leakage, the monitored persons cannot be identified and subsequently their personal data and sensitive information about them misused.

Summary

Electronic monitoring is used to check sentenced criminals, often also recidivists who are on the edge of the society. Nevertheless, they are always persons who are human beings and have their human rights and freedoms. Last but not least, they have the right to the protection of personal data and sensitive information about them and their privacy. In connection with this, persons living in the household with a sentenced criminal and persons coming into contact with them have also right to the protection of their personal data and sensitive information.
Electronic monitoring enters to a sentenced criminal's personal life in invasive way. Personal data and sensitive information are collected and subsequently processed, used and somehow stored in electronic or paper form. For this reason, it is essential that the data and information are lawfully acquired and secured, including through the use of anonymisation and pseudonymisation. It is also necessary that only persons designated by the law come into contact with this data.

Given the fact that the legislation, whether in the territory of the Slovak Republic or in the European area is not sufficiently elaborated in this area, it would be appropriate to fill this gap. Otherwise, electronic monitoring of sentenced criminals will not be carried out in accordance with the requirements for the protection of personal data and sensitive information and privacy and will violate fundamental rights and freedoms arising in particular from the EU Charter.

REFERENCES

1. Coordinated Artificial Intelligence Plan available on https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/sk/pdf
2. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
3. HUČKOVÁ, R. — SOKOL, P., RÓZENFELDOVÁ, L.: 4th industrial revolution and challenges for european law (with special attention to the concept of digital single market). In: EU and comparative law issues and challenges series : Eu law in context — adjustment to membership and challenges of the enlargement : International Scientific Conference. — Osijek : Sveučilište Josipa Jurja Strossmayera u Osijeku, 2018

4. General Regulation of the European Parliament and of the Council (EU) from 27th of 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
5. KLÁTIK, J.. Uplatňovanie restoratívnej justície a elektronického monitoringu na Slovensku a vo vybraných štátoch Európskej únie. I. KOŠICKÉ DNI TRESTNÉHO PRÁVA — Perspektívy vývoja európskeho trestného práva. Košice, 2018. Univerzita Pavla Jozefa Šafárika v Košiciach
6. MIHÓK, P.: Vybrané právne a etické aspekty umelej inteligencie pri elektronickom monitoringu obvinených a odsúdených osôb. In. SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.): *Právo, obchod, ekonomika IX.* Košice: Univerzita P. J. Šafárika v Košiciach, 2019
7. RAJNIČ, M.: Trest domáceho väzenia v systéme trestov. Justičná revue, 61, 2009, č. 6-7
8. The Recommendation CM / Rec (2014) 4 of the Committee of Ministers of the Member States on electronic monitoring
9. TÓTHOVÁ, V., FERENČÍKOVÁ, S. (2019). INNOVATION IN CRIMINAL POLICY OF IMPOSING ALTERANTIVE SANCTIONS IN SLOVAK REPUBLIC. In P. Hájek, & O. Vít (Ed.), CBU International Conference Proceedings. 7, pp. 661-670. Prague: CBU Research Institute
10. VESELÝ, P.: Pseudonymizácia a anonymizácia osobných údajov ako požiadavka GDPR, https://www.zoou.sk/33/pseudonymizacia-a-anonymizacia-osobnych-udajov-ako-poziadavka-gdpr-uniqueidmRRWSbk196FPkyDafLfWAJWc7pG-Xzb6XqJG803ba64/
11. ŽUĽOVÁ, J. 2018. Profilovanie a automatizované rozhodovanie (nielen) v pracovnoprávnych vzťahoch. In ŠVEC, M. — BULLA, M. (eds). *Práca 4.0, digitálna spoločnosť a pracovné právo [online]. [citované 06.09.2019].* Bratislava: Friedrich Ebert Stiftung